IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Singh	
U.S. Patent No.:	**8,904,030**	**Attorney Docket No.: 50048-0060IP1**
Issue Date:	December 2, 2014	
Appl. Serial No.:	14/295,353	
Filing Date:	June 4, 2014	
U.S. Patent No.:	**9,900,766**	**Attorney Docket No.: 50048-0056IP1**
Issue Date:	February 20, 2018	
Appl. Serial No.:	15/640,594	
Filing Date:	July 3, 2017	
U.S. Patent No.:	**11,234,121**	**Attorney Docket No.: 50048-0055IP1**
Issue Date:	January 25, 2022	
Appl. Serial No.:	16/532,507	
Filing Date:	August 6, 2019	
U.S. Patent No.:	**11,659,381**	**Attorney Docket No.: 50048-0054IP1**
Issue Date:	May 23, 2023	
Appl. Serial No.:	17/542,373	
Filing Date:	December 4, 2021	
Title:	**AUTOMATIC MULTIMEDIA UPLOAD FOR PUBLISHING DATA AND MULTIMEDIA CONTENT**	

DECLARATION OF DAVID B. LETT

TABLE OF CONTENTS

I. BACKGROUND 4
II. QUALIFICATIONS 5
III. MATERIALS CONSIDERED 10
IV. UNDERSTANDING OF THE LAW 14
A. Legal Standard for Prior Art 14
B. Legal Standard for Anticipation 14
C. Legal Standard for Obviousness 15
D. Legal Standard for Written Description 19
V. Overview of Background Technology 20
A. Digital Cameras 20
B. Bluetooth (BT) 23
C. HTTP 36
VI. The Challenged Patents 37
A. Overview of the Challenged Patents 37
B. Summary of the Common Disclosure 40
C. Summary of Prosecution History 48
D. Claim Construction 52
E. Person of Ordinary skill in the art 53
VII. Priority Analysis 53
A. The challenged claims of the ’766, ’121, and ’381 patents mix and match features from different systems. 54
B. The ’030 patent does not describe elements of the claimed inventions 65
VIII. Summary of the Prior Art 67
A. Hiroishi 67
B. Takahashi 69
C. Kahn 71
D. Endsley 72
E. Feinberg 72

IX. Overview of the Grounds 73
XI. Invalidity Analysis of The ’030 Patent.....75
A. Ground 1A – Hiroishi in combination with Takahashi and Bluetooth V2.1 Renders Claims 1-2, 4-7, 9-18 Invalid.....75
B. Ground 1B—Hiroishi in Combination with Kahn and Bluetooth 2.1 Renders Claims 1-18 Invalid 144
C. Ground 2A—Claims 1-14 are obvious over Singh129 in view of Bluetooth 209
D. Ground 2B—Claims 15-18 are obvious over Singh129 in view of Bluetooth and Takahashi 223
XII. Invalidity Analysis of the ’766 patent 227
A. Ground 1: Singh129 renders claims 1-15 obvious 227
B. Ground 2A: Kahn in view of Bluetooth renders claims 1-15 obvious.....248
C. Ground 2B: Kahn in view of Feinberg and Bluetooth renders claims 1-15 obvious 369
XIII. Invalidity Analysis of the ’121 Patent 486
A. Ground 1: Hiroishi in view of Kahn, Endsley, and Bluetooth renders claims 1-10 obvious.....487
B. Ground 2: Singh129 renders claims 1-10 obvious 588
XIV. Invalidity Analysis of the ’381 patent 611
A. Ground 1: The Combination of Hiroishi and Kahn Render Claims 1-16 Obvious 611
B. Ground 2: Singh129 renders claims 1-16 obvious 668
XVI. CONCLUSION.....688
XVII. APPENDIX.....689
A. ‘030 CLAIMS LISTING 689
B. ‘766 CLAIMS LISTING 701
C. ‘121 CLAIMS LISTING 715
D. ‘381 CLAIMS LISTING 729

I, David B. Lett, of Duluth, Georgia, declare that:

I. BACKGROUND

1. My name is David B. Lett, and I have been retained on behalf of TikTok Inc. to offer technical opinions relating to U.S. Patent Numbers 8,904,030 ("the '030 patent"), 9,900,766 ("the '766 patent"), 11,234,121 ("the '121 patent"), and 11,659,381 ("the '381 patent") (together, "the Challenged Patents") and prior art references relating to its subject matter. My experience with digital multimedia, wireless communications, and web application technologies provides me with an understanding of the subject matter described and claimed in the Challenged Patents.

2. My opinions, as explained below, are based on my education, experience, and expertise in the fields relating to the Challenged Patents. Any figures that appear within this document have been prepared with the assistance of Counsel and reflect my understanding of the Challenged Patents and the prior art discussed below.

3. I have no financial interest in the party or in the outcome of this proceeding. I am being compensated for my work as an expert on an hourly basis. My compensation is not dependent on the outcome of these proceedings or the content of my opinions.

II. QUALIFICATIONS

4. I am a technical consultant and product development industry veteran with expertise in electronics, software, hardware, video, audio, and data communications (including wireless cellular and Bluetooth), having led product development organizations in cable, satellite, consumer electronics, asset tracking, remote tank logistics, and alarm industries. My current *curriculum vitae* is attached as Appendix A and some highlights follow.

5. I earned my B.S. in Electrical Engineering (1982) with high honors from the University of Tennessee in Knoxville, Tennessee. I also attended the Georgia Institute of Technology from 1986 to 1987, completing 40% of the required degree hours for the M.S. Electrical Engineering program,

6. From 1982 to 1985, I worked at Scientific Atlanta as an Electrical Engineer designing video, audio, and data communications equipment for the cable television industry. I designed software and hardware including addressable data transmitters, video sync suppression scramblers, transaction format converters, and data channel monitors for addressable Cable Television systems and Set Top Boxes.

7. From 1983 to 1985, while working at Scientific Atlanta, I also worked as an Assistant Professor at DeVry Institute of Technology, teaching courses in electronics and microprocessor hardware/software.

8. From 1985 to 1990, I worked at Wegener Communications as a Senior Electrical engineer, designing satellite communications equipment including forward error correction (FEC) coding systems, PSK modems, and analog control systems for RF modulators and PSK demodulators. I was promoted to the Hardware Engineering Manager, where I managed product development of video, audio, and data satellite receivers, modulators, graphics display systems, DSP-based compandors, FSK and PSK satellite modems, multiplexers, forward error correction (FEC) codecs, RF upconverters and downconverters, and baseband analog and digital processing components.

9. In 1990, I returned to Scientific Atlanta, which was acquired by Cisco in 2006. I worked as Engineering Manager running the set top box engineering group where I was promoted to Director and Vice President during my tenure until 2011. I led the design of many cable set top boxes and systems through the evolution of analog video, addressability, downloadable software, electronic program guides, digital video, software applications, high-definition TV, DVR, DOCSIS, full spectrum tuners, and multiroom DVR. These systems implemented various technologies including DOCSIS 1/2/3 and hybrid gateways, 802.11, IPTV, DVR, cable modems, ADSL, VDSL, DVB-T/C/S, bootloaders, factory diagnostics, application frameworks, Nagra, DRMs, conditional access, secure microprocessors, device management, Android, Adobe Flash, Linux, DVD

play/record, MPEG-4, MPEG-2, H.264, NTSC, PAL, DAVIC, MoCA, high-performance CPUs, cablecards, network processors, HDMI, multiple video/audio display interfaces, 2D/3D graphics, and multiple RF tuners.

10. From 2011 to 2016, I worked for EchoStar Technologies, which served as the product development organization for sister company DISH Network. I served as Vice President of Engineering and was the Head of the Atlanta research and development center. I led the development of satellite set top boxes, consumer electronic equipment, and a home automation and security system. Technologies used included video/audio, IoT, H.265, HEVC, 3D, Satellite, wireless Zigbee, Z-Wave, Wi-Fi, Bluetooth, MoCA, transcoding, embedded C Linux applications, mobile applications (IOS and Android), SaaS, web applications (JavaScript, HTML), BSS/OSS, AWS cloud storage, 2-way video/audio streaming, authentication, and VoIP.

11. In 2016, I started an independent consulting business in technology and intellectual property projects. I have consulted in various technology areas and industries including consumer electronics, cable, satellite, television, security, camera image/AV capture and processing, online advertising, and Internet of Things (IoT).

12. From 2019 to 2022, I worked as Chief Technology Officer for Telular, an Ametek company. I was responsible for the development of Industrial

IoT (IIoT) recurring revenue solutions, combining wireless technologies (cellular, Bluetooth, sub-GHz, GPS, and satellite), purpose-built hardware, and SaaS in the commercial telematics, security and home automation markets and sold under the SkyBitz and Telguard Brands.

13. My record of professional service includes awards on products I designed and developed from several organizations in my field of expertise, including Best of Show, Technology Emmy, and Best of Innovations.

14. I am a named inventor on at least 117 issued patents and published patent applications corresponding to the areas of my professional work. The patents and published applications involving data communications and multimedia technologies include:

- U.S. Patent No. 9,615,139 titled "Determining Device That Performs Processing of Output Pictures"
- U.S. Patent No. 9,495,860 titled "False Alarm Identification" Pictures"
- PCT Patent Publication No. WO 2022/231962 titled "Tractor-trailer id methods and system"
- U.S. Patent No. 9,882,736 titled "Remote Sound Generation for a Home Automation System"
- European Patent No. EP 1,552,698 titled "Video transmission systems and methods for a home network"

- U.S. Patent Nos. 8,120,924, 7,240,217, 6,785,817, 6,564,324, 6,212,278 and 5,440,632 titled "Reprogrammable subscriber terminal"

- U.S. Patent Application No. US2015/0160636 titled "Multi-Tiered Feedback-Controlled Home Automation Notifications"

- U.S. Patent Nos. 9,247,409 and 9,691,261 titled "Home Automation Communications"

- U.S. Patent No. 10,063,641 titled "Systems and methods for finding wireless signals sufficient for installation of wireless home automation devices"

- U.S. Patent No. 5,657,414 titled "Auxiliary device control for a subscriber terminal"

- PCT Patent Publication No. WO 2003/083606 titled "Exporting data from a digital home communication terminal to a client device"

- U.S. Patent No. 8,549,567 titled "Media Content Sharing Over a Home Network"

- U.S. Patent No. 8,161,388 titled "Interactive discovery of display device characteristics"

- U.S. Patent No. 7,908,625 titled "Networked Multimedia System"

- U.S. Patent Nos. 7,861,272 and 7,849,486 titled "Networked subscriber television distribution"

- U.S. Patent Nos. 7,774,820 and 7,069,578 titled "Settop cable television control device and method including bootloader software and code version table for maintaining and updating settop receiver operating system software"

- U.S. Patent No. 5,715,515 titled "Method and apparatus for downloading on-screen graphics and captions to a television terminal"

- U.S. Patent No. 5,592,551 titled "Method and apparatus for providing interactive electronic programming guide"

- U.S. Patent No. 5,539,822 titled "System and Method for Subscriber Interactivity in a Television System"

- U.S. Patent Application Publication Nos. 2004/0068753 and 2008/0072272 titled "Video Transmission Systems and Methods for a Home Network"

- U.S. Patent No. 5,771,064 titled "Home communications terminal having an applications module"

- U.S. Patent Application Publication No. 2004/0133911 titled "Subscriber Network in a Satellite System"

- U.S. Patent No. 5,367,571 titled "Subscriber terminal with plug in expansion card"

- U.S. Patent No. 5,357,276 titled "Method of Providing Video On Demand with VCR Like Functions"

- U.S. Patent No. 4,817,148 titled "Signal scrambling transmission system"

III. MATERIALS CONSIDERED

15. I have reviewed the Challenged Patents and relevant excerpts of the prosecution history of the Challenged Patents. I have also reviewed the materials that the Challenged Patents allegedly incorporate by reference (specifically, U.S. Patent Application No. 11/901802 ("the '802 application"), published as U.S. Patent Publication 2008/0103906 ("the '906 publication"). I have also reviewed the petitions and institution decisions for two previous IPRs concerning U.S.

9,258,698 ("the '698 patent"), which was invalidated by the PTAB. *See* IPR2019-00127; IPR2019-00131. I have also reviewed the following prior art references and materials, in addition to other materials I cite in my declaration:

- U.S. 8,904,030 (TTI-1001)
- Excerpts from the '030 patent File History (TTI-1002)
- U.S. 9,900,766 (TTI-1003)
- Excerpts from the '766 patent File History (TTI-1004)
- U.S. 11,234,121 (TTI-1005)
- Excerpts from the '121 patent File History (TTI-1006)
- U.S. 11,659,381 (TTI-1007)
- Excerpts from the '381 patent File History (TTI-1008)
- U.S. Publication 2009/0172129 ("Singh129" or TTI-1009)
- U.S. Publication 2008/0103906 ("Singh906" or TTI-1010)
- Certified Translation of JP 2003-60953 ("Hiroishi" or TTI-1011)
- Certificate of Translation for Hiroishi (TTI-1012)
- Original Japanese Publication of Hiroishi (TTI-1013)
- Certified Translation of JP 2005-303511 ("Takahashi" or TTI-1014)
- Certificate of Translation for Takahashi (TTI-1015)
- Original Japanese Publication of Takahashi (TTI-1016)
- U.S. Publication 2004/0004737 ("Kahn" or TTI-1017)

- U.S. 8,385,950 (“Wagner” or TTI-1018)
- Bluetooth ™ Core Specification 2.1 + EDR (“Bluetooth” or “Bluetooth Core Specification V2.1” or TTI-1019)
- U.S. 6,636,259 (“Anderson” or TTI-1020)
- U.S. 7,639,943 (“Kalajan” or TTI-1021)
- U.S. Pub. 2006/0173985 (“Moore” or TTI-1022)
- U.S. Pub. 2006/0143684 (“Morris” or TTI-1023)
- U.S. Pub. 2006/0139474 (“Endsley” or TTI-1024)
- U.S. Pub. 2007/0073937 (“Feinberg” or TTI-1025)
- U.S. Patent Application No. 11/901,802 (“Singh906 Application” or TTI-1026)
- U.S. Pub. 2002/0046249 (“Shiigi” or TTI-1029)
- Archived Webpage Bluetooth™ Core Specification v2.1 + EDR (https://web.archive.org/web/20071011031607/http:/bluetooth.com/Bluetooth/Learn/Technology/Specifications/Default.htm) (TTI-1031)
- C. Bisdikian, “An overview of the Bluetooth wireless technology,” in IEEE Communications Magazine, vol. 39, no. 12, pp. 86-94, Dec. 2001, doi: 10.1109/35.968817. (“The Bluetooth Overview” or TTI-1032)
- Excerpts from the Prosecution History of U.S. Patent App. No. 14/503,401 (TTI-1033)

- Patent Owner's Preliminary Infringement Contentions (TTI-1036)

IV. UNDERSTANDING OF THE LAW

A. Legal Standard for Prior Art

16. I understand that a patent or other publication must first qualify as prior art before it can be used to invalidate a patent claim.

17. I understand that a patent or other publication is prior art if it was patented or published anywhere in the world before the Applicant's earliest filing date. I understand that a US patent or published US patent application is prior art if it was by someone other than the named inventor of the challenged patent and was filed before the Applicant's earliest filing date.

18. I understand that to qualify as prior art, a reference must contain an enabling disclosure that allows one of ordinary skill in the art (a "skilled artisan") to practice the claims without undue experimentation.

19. I understand that prior art can be used to invalidate a patent claim as anticipated or as obvious.

B. Legal Standard for Anticipation

20. I have been instructed by counsel that a patent claim is invalid as anticipated if each and every element of a claim, as properly construed, is found either explicitly or inherently in a single prior art reference. Under the principles of inherency, I understand that if the prior art necessarily functions in accordance with, or includes the claimed limitations, it anticipates.

21. I understand that a prior art reference may incorporate material by

reference and the effect of incorporation is that the incorporated material is effectively part of the host document as if it were explicitly contained within it.

22. I have written this declaration with the understanding that in an *inter partes* review anticipation must be shown by a preponderance of the evidence.

C. Legal Standard for Obviousness

23. I have been instructed by counsel on the law regarding obviousness, and understand that even if a patent is not anticipated, it is still invalid if the differences between the claimed subject matter 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 skilled artisan in the pertinent art.

24. I understand that the understanding and knowledge of a skilled artisan at the time of the invention provides a reference point from which the prior art and claimed invention should be viewed. This reference point prevents the use of hindsight in deciding whether a claim would have been obvious to a skilled artisan.

25. I also understand that an obviousness determination includes the consideration of various factors such as (1) the scope and content of the prior art, (2) the differences between the prior art and the challenged claims, (3) the level of ordinary skill in the pertinent art, and (4) the existence of secondary considerations such as (i) a long felt but unmet need in the prior art that was satisfied by the invention of the patent; (ii) commercial success or lack of commercial success of

processes covered by the patent; (iii) unexpected results achieved by the invention; (iv) praise of the invention by others skilled in the art; (v) taking of licenses under the patent by others; and (vi) deliberate copying of the invention. I also understand that there must be a relationship between any such secondary indicia and the invention. I further understand that contemporaneous and independent invention by others is a secondary consideration supporting an obviousness determination.

26. I understand that an obviousness may be based on a single prior art reference or a combination of multiple references. I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but that the reason need not be found in the references themselves and may come from common sense or other knowledge in the art.

27. I understand that if a technique has been used to improve one device, and a skilled artisan would recognize that it would improve similar devices in the same way, using the technique would have been obvious unless its actual application is beyond his or her skill.

28. I also understand that practical and common-sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. I further understand that a skilled artisan looking to overcome a problem will often be able to fit the teachings of multiple publications together like pieces of a puzzle, although the prior art need

not be like two puzzle pieces that must fit perfectly together. I understand that obviousness analysis therefore considers the inferences and creative steps that a skilled artisan would employ under the circumstances.

29. I understand that a particular combination may be proven obvious by showing that it was obvious to try the combination. For example, when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a skilled artisan has good reason to pursue the known options within his or her technical grasp because the result is likely the product not of innovation but of ordinary skill and common sense.

30. I understand that the combination of familiar elements according to known methods may be proven obvious when it does no more than yield predictable results. When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a skilled artisan can implement a predictable variation, obviousness likely bars its patentability.

31. It is further my understanding that a proper obviousness analysis focuses on what was known or obvious to a skilled artisan, not just the patentee. Accordingly, I understand that any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

32. I understand that a claim can be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found explicitly or inherently in the reference can be supplied by the common sense of one of skill in the art.

33. I understand that a skilled artisan could have combined two pieces of prior art or substituted one prior art element for another if the substitution can be made with predictable results, even if the swapped-in element is different from the swapped-out element. In other words, the prior art need not be like two puzzle pieces that must fit together perfectly. The relevant question is whether prior art techniques are interoperable with respect to one another, such that that a person of skill would view them as a design choice, or whether a person of skill could apply prior art techniques into a new combined system.

34. In sum, my understanding is that prior art teachings are properly combined where a skilled artisan having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claims. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor at the time of the invention, can provide a reason for combining the elements of multiple prior art references in the claimed manner.

35. I have been informed and understand that the obviousness analysis

requires a comparison of the properly construed claim language to the prior art on a limitation-by-limitation basis.

36. I have written this declaration with the understanding that in an inter partes review obviousness must be shown by a preponderance of the evidence.

D. Legal Standard for Written Description

37. I understand that, to rely on the filing date of an earlier application, the earlier application must include a disclosure that complies with the written description requirement.

38. I understand that the written description requirement is separate and distinct from the enablement requirement.

39. I understand that the goal of the written description requirement is to clearly convey that an applicant has invented the subject matter claimed and to guard against the inventor's overreaching by insisting that the inventor recount the claimed invention in such detail that future claims can be determined to be encompassed within the inventor's original creation. I understand that another goal of the written description requirement is to convey to the public what the applicant claims as the invention.

40. I understand that, to comply with the written description requirement, the specification must describe the invention sufficiently to convey to a person of skill in the art that the patentee had possession of the claimed invention at the time

of the application, *i.e*., that the patentee invented what is claimed. I further understand that the disclosure as originally filed does not have to provide word for word support for the claimed subject matter at issue. However, a person of ordinary skill in the art, reading the original specification, must immediately discern the claimed invention.

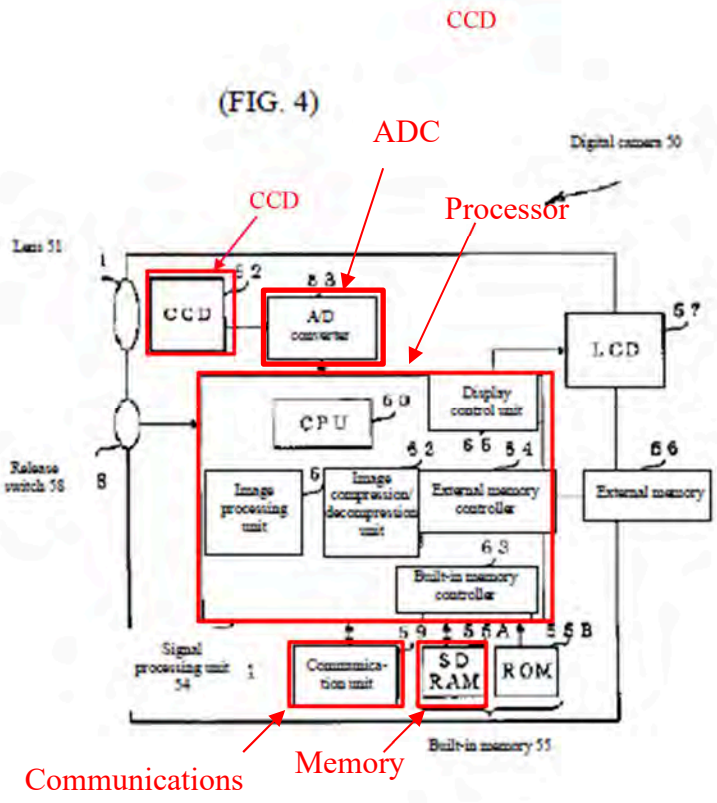
41. I understand that entitlement to an earlier filing date extends only to the subject matter that is disclosed; not to that which is obvious. Accordingly, I understand that the question is not whether a person skilled in the art might be able to construct the claimed subject matter from the teachings of the disclosure. Instead, the question is whether the application necessarily discloses that particular device.

42. I understand that one cannot disclose a forest in the original application, and then later pick a tree out of the forest and say here is my invention. Instead, to satisfy the written description requirement, there must be blaze marks in the priority application directing a person of ordinary skill in the art to a specific tree. In other words, I understand that the patent must inform a person of ordinary skilled in the art that the inventors contemplated the specific combination of elements recited in the challenged claims.

V. OVERVIEW OF BACKGROUND TECHNOLOGY

A. Digital Cameras

43. Digital cameras capture photos using a solid-state image sensor, as opposed to a non-digital camera that use traditional film. *See, e.g.*, TTI-1017, [0006]-[0007], [0039]. The typical main components of a digital camera are the lens, shutter, image sensor, ADC, processor (microprocessor) and associated components, memory, user interface (display, controls), and various interfaces to other devices. *See, e.g.*, *id*., [0037]-[0048]; TTI-1011, [0055]-[0065]. One such embodiment of a digital camera is shown below in FIG. 4 from Hiroishi, TTI-1011. Hiroishi's digital camera 50 uses a charge-coupled device (CCD) sensor 52 image sensor. *See, e.g.*, TTI-1011, [0055]. The communications unit 59 provides an interface to other devices. *See, e.g.*, *id*., [0058], [0067]. FIG. 4 is reproduced below:



Hiroishi, FIG. 4 (annotated)

44. Likewise, Kahn's digital camera also includes a communication interface (I/O controller 280, shown in FIG. 2B). The "I/O controller 280 is an interface device allowing communications to and from the computer 140" and permits an external host, such as a cell phone "to connect to and communicate with the computer 140" of the digital camera. TTI-1017, [0045].

45. These communication interfaces to other devices (such as communications interface 59 or I/O controller 280) can be wired or wireless and are the biggest advantage of digital cameras as "compared to a traditional film cameras, making it easy to transfer images between all kinds of devices and

applications." TTI-1017, [0006], [0055] ("The camera device 310 is preferably a wireless camera device, such as camera device 100 (shown in FIG. 1A), that either includes wireless connectivity itself or connects to a local host with wireless connectivity."); see also TTI-1011, [0066]-[0067]. Thus, digital cameras had have become "increasingly popular" by the alleged Critical Date of the subject patents. *See, e.g.*, TTI-1017, [0006].

46. One popular wireless interface used on digital cameras is Bluetooth, allowing transfer of images and associated data / metadata (location, user ID, timestamp, etc.) and remote control of the camera possible without any cables on this short range wireless and cryptographically secure interface. As such, Hiroishi's digital camera embodiment in FIG. 4 uses Bluetooth for the Communications unit 59. TTI-1017, [0006]-[0009], TTI-1011, [0066]-[0067].

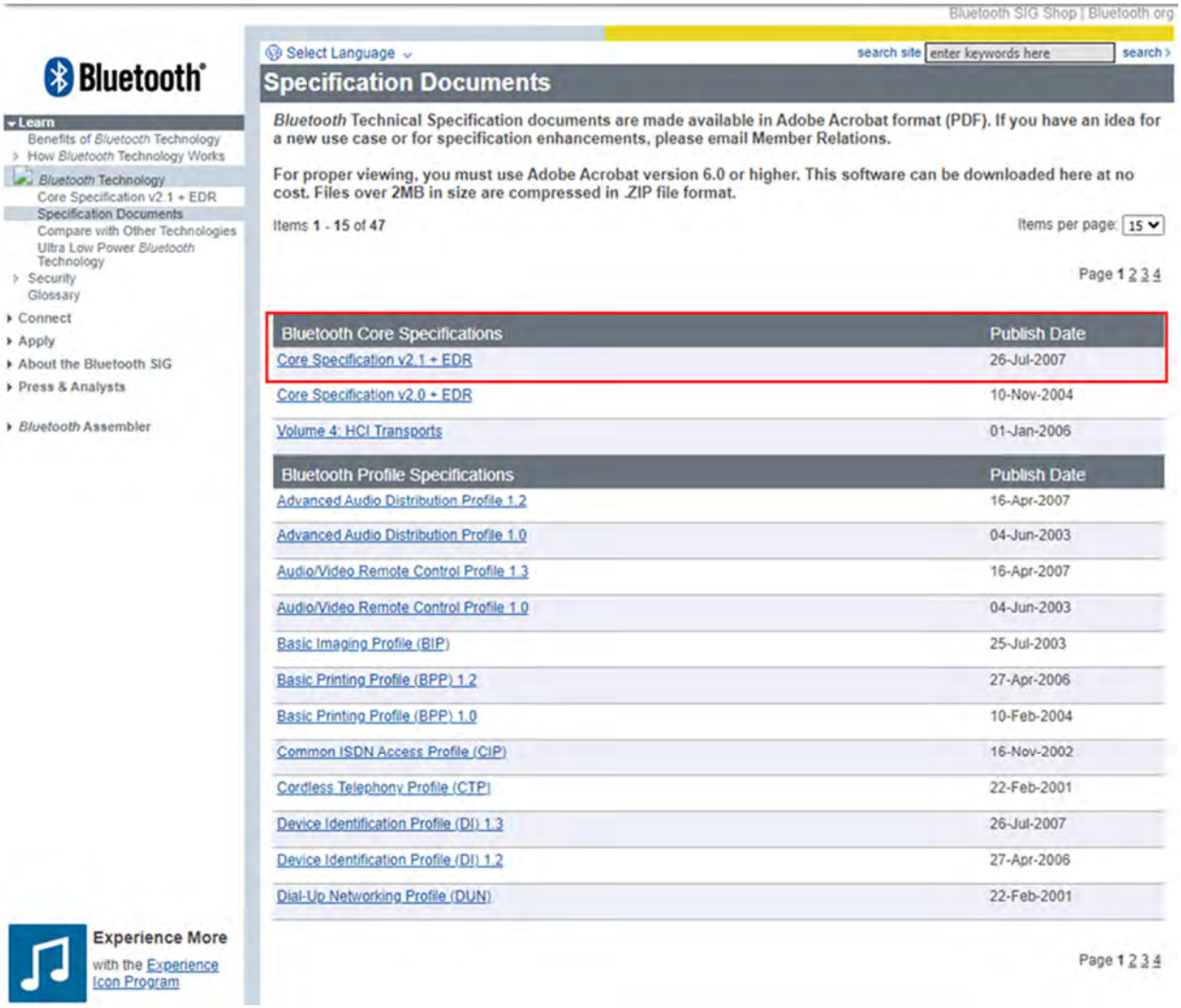
B. Bluetooth (BT)

47. As of December 28, 2007, (the alleged Critical Date of the challenged patents) Bluetooth (BT) had been widely adopted and prevalent as the go-to standard for devices to communicate using short-range point-point RF communications in many applications including consumer electronics, like communication between a camera and a mobile devices (e.g., cellular telephone). TTI-1032, 1-2. Bluetooth has become popular for many reasons including the ease of pairing devices, prevalence of compatible devices, low power consumption,

encryption of communications, flexibility of data packet use, and the availability of design components (chipsets, ASIC cores, and software drivers/support). *Id.* The Bluetooth specification evolved through many versions/revisions from the initial Version 0.7 in 1998 to the current version as of the alleged Critical Date, Version 2.1 + EDR released July 26, 2007, and is thus prior art. TTI-1019, 1, 46-47. In addition, Bluetooth wireless technology (BT), had established its role in replacing cables for personal device interconnectivity and facilitating spontaneous communication between devices within a localized "communications bubble." TTI-1032, 1-2. The Bluetooth Overview discloses that Bluetooth's aim was to provide a universal, user-friendly interface for data services, enabling ad hoc connectivity and serving as a personal gateway for accessing remote services while maintaining convenience and privacy. TTI-1032, 1-2; TTI-1019, 1, 46-47. "Connecting to data services through one's cellular phone gives rise to the concept of a personal gateway. People will carry their personal gateways wherever they go." TTI-1032, 1.

48. Bluetooth technology was available before the alleged Critical Date of the patent, as supported by various pieces of evidence. TTI-1019, 1. First, the face of the Bluetooth Core Specification V2.1 provides publication date as July 26, 2007. Second, the same Bluetooth Core Specification V2.1 was provided as an exhibit by the Patent Owner in two IPR proceedings (IPR2019-00127 as Ex. 2018

and IPR2019-00131 as Ex. 2006), both involving U.S. Patent 9,258,698 (a family member of the '030 patent). Third, the WayBack Machine contains an archived webpage in October, 2007, confirming the publication of the Bluetooth Core Specification V2.1 on July 26, 2007, and its public accessibility by no later than October, 2007. TTI-1031, 1. The content of the page is credible as it mentions Bluetooth 2.1 as the latest available release and thus predates the release of Bluetooth 2.2.



TTI-1031, 1 (annotated). Finally, the ’030 patent relies on pre-existing Bluetooth technology and thus acknowledges that Bluetooth is prior art. TTI-1001, 2:3.

49. As of the alleged Critical Date, Bluetooth wireless technology (BT), had established its role in replacing cables for personal device interconnectivity and facilitating spontaneous communication between devices within a localized “communications bubble.” TTI-1032, 1-2. The Bluetooth Overview discloses that Bluetooth’s aim was to provide a universal, user-friendly interface for data services, enabling ad hoc connectivity and serving as a personal gateway for accessing remote services while maintaining convenience and privacy. TTI-1032, 1-2.

50. The Bluetooth Core Specification describes the implementation of security at both the link layer and the application layer:

1 SECURITY OVERVIEW

Bluetooth wireless technology provides peer-to-peer communications over short distances. In order to provide usage protection and information confidentiality, the system provides security measures both at the application layer and the link layer. These measures are designed to be appropriate for a peer environment. This means that in each device, the authentication and encryption routines are implemented in the same way. Four different entities are used for maintaining security at the link layer: a Bluetooth device address, two secret keys, and a pseudo-random number that shall be regenerated for each new transaction. The four entities and their sizes are summarized in Table 1.1.

Entity	Size
BD_ADDR	48 bits
Private user key, authentication	128 bits
Private user key, encryption configurable length (byte-wise)	8-128 bits
RAND	128 bits

Table 1.1: Entities used in authentication and encryption procedures.

The Bluetooth device address (BD_ADDR) is the 48-bit address. The BD_ADDR can be obtained via user interactions, or, automatically, via an inquiry routine by a device.

The secret keys are derived during initialization and are never disclosed. The encryption key is derived from the authentication key during the authentication process. For the authentication algorithm, the size of the key used is always 128 bits. For the encryption algorithm, the key size may vary between 1 and 16 octets (8 - 128 bits). The size of the encryption key is configurable for two reasons. The first has to do with the many different requirements imposed on cryptographic algorithms in different countries – both with respect to export regulations and official attitudes towards privacy in general. The second reason is to facilitate a future upgrade path for the security without the need of a costly redesign of the algorithms and encryption hardware; increasing the effective key size is the simplest way to combat increased computing power at the opponent side.

See, e.g., TTI-1019, 1025.

51. The BT specification describes cryptographically authenticating devices for pairing, the pairing process aimed at creating a shared secret, i.e. a Link Key to authenticate devices to each other and encrypt exchanged data. *See, e.g.*, TTI-1019, 131-132, 1058-1071 (describing Secure Simple Pairing), 1317 (describing LMP pairing). There were two methods, the first being LMP Pairing

(PIN-code based) and the second being the Secure Simple Pairing (SSP) processes. The data is actually not directly encrypted with the Link Key; a temporary Encryption Key is derived from the Link Key and from random numbers that are exchanged shortly before the start of the encrypted traffic. This Encryption Key is then used for encrypting the data in both directions. It can be changed at any time while the connection is active and will be discarded as soon as the connection is closed, or if the encryption is stopped.

52. The first cryptographic authentication method, LMP pairing (PIN code based) uses the BD_ADDR to form a common the initialization key (Kinit):

4.2.2 Pairing

When two devices do not have a common link key an initialization key (K_{init}) shall be created based on a PIN, and a random number and a BD_ADDR. K_{init} shall be created as specified in [Part H] Section 6.3 on page 805. When both devices have calculated K_{init} the link key shall be created, and a mutual authentication is performed. The pairing procedure starts with a device sending an LMP_in_rand PDU; this device is referred to as the "initiating LM" or "initiator" in Section 4.2.2.1 on page 251 - Section 4.2.2.5 on page 253. The other device is referred to as the "responding LM" or "responder". The PDUs used in the pairing procedure are:

M/O	PDU	Contents
M	LMP_in_rand	random number
M	LMP_au_rand	random number
M	LMP_sres	authentication response
M	LMP_comb_key	random number
M	LMP_unit_key	key

Table 4.13: PDUs used for pairing

All sequences described in Section 4 on page 233, including the mutual authentication after the link key has been created, shall form a single transaction. The transaction ID from the first LMP_in_rand shall be used for all subsequent sequences.

TTI-1019, 412.

4.2.2.4 Creation of the link key

When K_{init} is calculated in both devices the link key shall be created. This link key will be used in the authentication between the two devices for all subsequent connections until it is changed; see Section 4.2.3 on page 245 and Section 4.2.4 on page 246. The link key created in the pairing procedure will either be a combination key or one of the device's unit keys. The following rules shall apply to the selection of the link key:

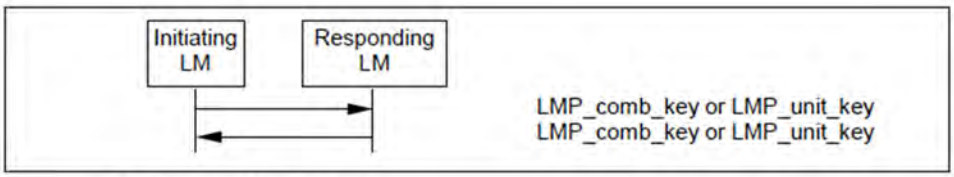
- if one device sends an LMP_unit_key PDU and the other device sends LMP_comb_key, the unit key will be the link key.
- if both devices send an LMP_unit_key PDU, the master's unit key will be the link key.
- if both devices send an LMP_comb_key PDU, the link key shall be calculated as described in [Part H] Section 3.2 on page 861.

The content of the LMP_unit_key PDU is the unit key bitwise XORed with K_{init}. The content of the LMP_comb_key PDU is LK_RAND bitwise XORed with K_{init}. Any device configured to use a combination key shall store the link key.

The use of unit keys is deprecated since it is implicitly insecure.

When the new link key has been created mutual authentication shall be performed to confirm that the same link key has been created in both devices. After mutual authentication, the initiating device shall pause and immediately resume encryption to produce a new encryption key. Note that this will cause a new encryption key to be generated from the ACO created during the mutual authentication process, and the random number sent in the LMP_start_encryption_req PDU which occurs in response to the resumption of encryption.

After mutual authentication, if encryption is enabled, the initiating device shall pause and immediately resume encryption to produce a new encryption key. Note that this will cause a new encryption key to be generated from the ACO created during the mutual authentication process, and the random number sent in the LMP_start_encryption_req PDU which occurs in response to the resumption of encryption.



Sequence 28: Creation of the link key.

TTI-1019, 414-415.

53. The second cryptographic authentication pairing method, Secure Simple Pairing, was introduced into the specification as a new feature in Bluetooth Core Specification 2.1 + EDR to simplify the pairing process and to improve security. TTI-1019, 154. Secure Simple Pairing uses a much more elaborate mechanism, known as elliptic curve cryptography to improve security, e.g. to avoid man-in-the middle attacks. TTI-1019, 131-132. The specification describes the obvious reasons for secure pairing and the secure simple pairing process:



BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 1] page 57 of 96

Architecture

Bluetooth

5 SECURE SIMPLE PAIRING OVERVIEW

The primary goal of Secure Simple Pairing is to simplify the pairing procedure for the user. Secondary goals are to maintain or improve the security in Bluetooth wireless technology. Since high levels of security and ease-of-use are often at opposite ends of the spectrum in many technologies and products, much care has been taken to maximize security while minimizing complexity from the end user's point of view.

5.1 SECURITY GOALS

Secure Simple Pairing has two security goals: protection against passive eavesdropping and protection against man-in-the-middle (MITM) attacks (active eavesdropping). It is a goal of Secure Simple Pairing to exceed the maximum security level provided by the use of a 16 alphanumeric PIN with the pairing algorithm used in Bluetooth Core Specification version 2.0 + EDR and earlier versions. Note that many Bluetooth devices compliant with Bluetooth Core Specification 2.0 + EDR and earlier versions use a 4-digit PIN or a fixed PIN of commonly known values significantly limiting the security on the link.

TTI-1019, 131.

7 SECURE SIMPLE PAIRING

The Secure Simple Pairing security functions and procedures are described in this section. In addition, a cryptographic analysis of each procedure is provided.

There are five phases of Secure Simple Pairing:

- Phase 1: Public key exchange
- Phase 2: Authentication Stage 1
- Phase 3: Authentication Stage 2
- Phase 4: Link key calculation
- Phase 5: LMP Authentication and Encryption

Phases 1, 3, 4 and 5 are the same for all protocols whereas phase 2 (Authentication Stage 1) is different depending on the protocol used. Distributed through these five phases are 13 steps.

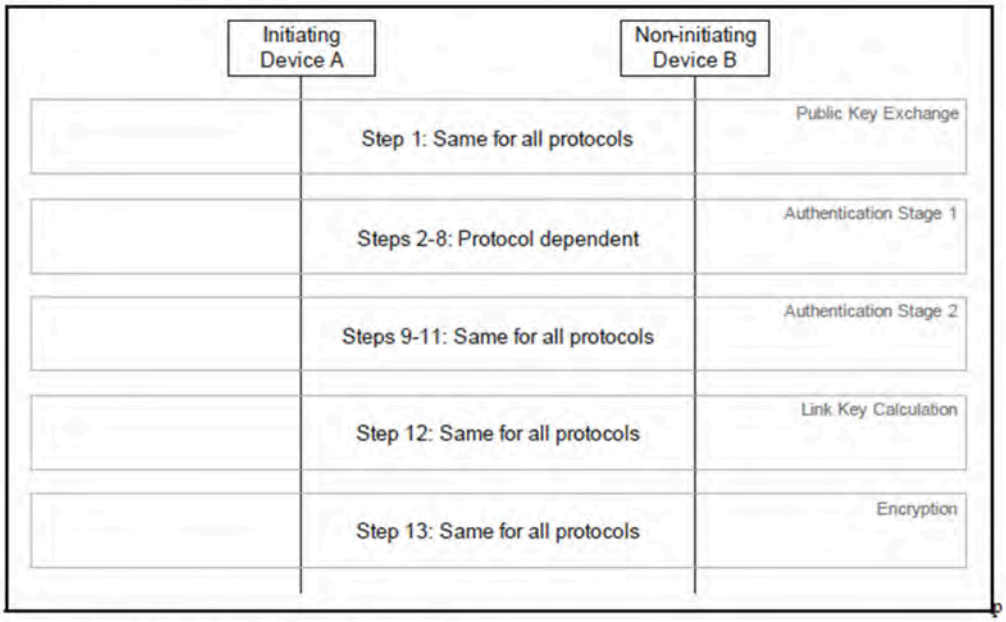


Figure 7.1: Simple Pairing Security Phases

TTI-1019, 1058-1071.

54. Cryptographic authentication between wireless devices like a digital camera and cellular phone was routine at the time of the invention. Indeed, cryptographic authentication using the first (LMP, PIN based) method described

was part of the Bluetooth standard for years before the alleged Critical Date of the subject patents.

55. The data packet format in Bluetooth allows data to be transported in each packet and are described in the specification, providing the flexibility to transport images and other payload as described in the subject patents.

56. BT also discusses polling as an example of event listening and notification. For example, polling is described in the active mode, i.e., where both the master and slave actively participate on the channel. TTI-1019, 331. Slaves in the active mode listen in the master-to-slave slots for packets.

> **8.6.1 Polling in the active mode**
>
> The master always has full control over the piconet. Due to the TDD scheme, slaves can only communicate with the master and not other slaves. In order to avoid collisions on the ACL logical transport, a slave is only allowed to transmit in the slave-to-master slot when addressed by the LT_ADDR in the packet header in the preceding master-to-slave slot. If the LT_ADDR in the preceding slot does not match, or a valid packet header was not received, the slave shall not transmit.
>
> The master normally attempts to poll a slave's ACL logical transport no less often than once every T_{poll} slots. T_{poll} is set by the Link Manager (see [Part C] Section 4.1.8 on page 234).
>
> The slave's ACL logical transport may be polled with any packet type except for FHS and ID. For example, polling during SCO may use HV packets, since the slave may respond to an HV packet with a DM1 packet (see Section 8.6.2 on page 162).

TTI-1019, 332.

In fact, the Bluetooth Core Specification defines a POLL type data packet that "does not have a payload", "requires a confirmation from the recipient", and "can be used by the master…to poll the slaves." TTI-1019, 283.

57. Another example of event listening and notification in the Bluetooth specification is sniff mode. Sniff mode is used to reduce power during an idle asynchronous connection as an alternative to constantly polling.

> **8.7 SNIFF MODE**
>
> In Sniff mode, the duty cycle of the slave's activity in the piconet may be reduced. If a slave is in active mode on an ACL logical transport, it shall listen in every ACL slot to the master traffic, unless that link is being treated as a scatternet link or is absent due to hold mode. With sniff mode, the time slots when a slave is listening are reduced, so the master shall only transmit to a slave in specified time slots. The sniff anchor points are spaced regularly with an interval of T_{sniff}.

TTI-1019, 345.

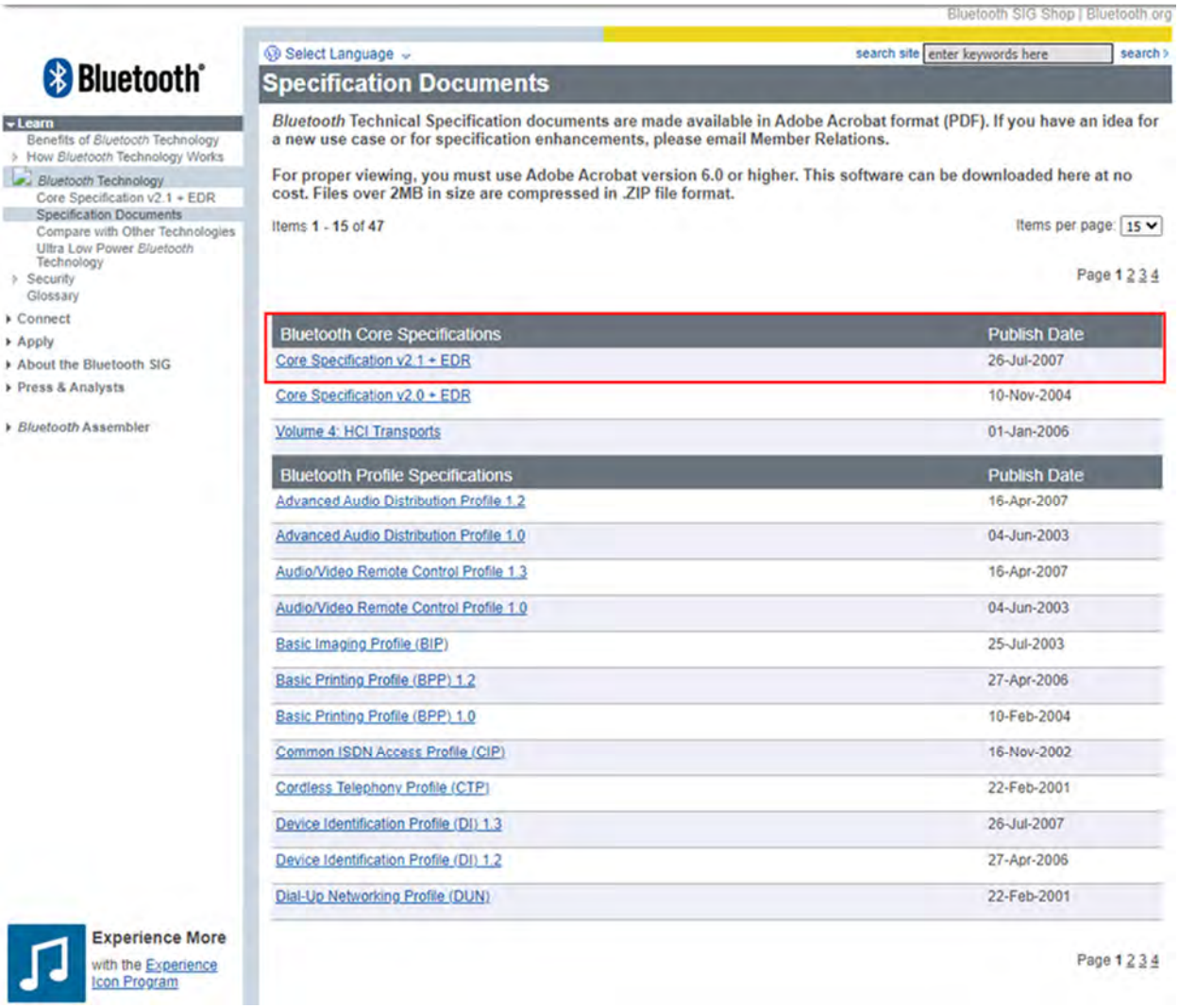
58. There is a clear process for enabling event listening using sniff mode.

> *4.5.3.1 Master or slave requests sniff mode*
>
> Either the master or the slave may request entry to sniff mode. The process is initiated by sending an LMP_sniff_req PDU containing a set of parameters. The receiving LM shall then decide whether to reject the attempt by sending an LMP_not_accepted PDU, to suggest different parameters by replying with an LMP_sniff_req PDU or to accept the request.

TTI-1019, 457.

59. Bluetooth technology was available before the alleged Critical Date of the patent, as supported by various pieces of evidence. TTI-1019, 1. First, the face

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



TTI-1031, 1 (annotated).

60. Finally, the ’381 patent relies on pre-existing Bluetooth technology and thus acknowledges that Bluetooth is prior art. TTI-1007, 2:25.

C. HTTP

61. HTTP (Hypertext Transfer Protocol) was a well-known and straightforward technique for uploading images to a website as of the alleged Critical Date of the subject patents. In fact, several publications disclose this

common application of HTTP, for example Kalajan, Takahashi, and Kahn. Kalajan teaches that a conventional HTTP POST request method can be used to upload images from the mobile device to Internet-connected servers and has many benefits as compared with other approaches. TTI-1021, 5:49-6:2. Takahashi also teaches uploading image data from a mobile device using HTTP. TTI-1016, [0005]-[0008]. Furthermore, Kahn discloses a mobile device uploading images to a website using HTTP., TTI-1017, [0056]. Therefore, a POSITA would understand that HTTP was a common and standard way to upload images from a cell phone over a cellular connection through the internet to a website.

VI. THE CHALLENGED PATENTS

A. Overview of the Challenged Patents

62. The Challenged Patents are titled Automatic Multimedia Upload for Publishing Data and Multimedia Content. *E.g.*, TTI-1001. There are several patents in this patent a family, four of which are subject to this declaration. A summary of the four Challenged Patents is as follows:

U.S. Patent No.:	**8,904,030**
Issue Date:	December 2, 2014
Appl. Serial No.:	14/295,353
Filing Date:	June 4, 2014
U.S. Patent No.:	**9,900,766**
Issue Date:	February 20, 2018
Appl. Serial No.:	15/640,594
Filing Date:	July 3, 2017
U.S. Patent No.:	**11,234,121**
Issue Date:	January 25, 2022
Appl. Serial No.:	16/532,507
Filing Date:	August 6, 2019
U.S. Patent No.:	**11,659,381**
Issue Date:	May 23, 2023
Appl. Serial No.:	17/542,373
Filing Date:	December 4, 2021

63. Each patent claims various aspects of a photographic 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." *E.g.*, '303 Patent, Abstract.

64. A summary of the claims of each of the Challenged Patents is as follows:

The '030 Patent Claims Summary
1. A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device

6. A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device
12. A method for transferring data to a remote internet server by a Bluetooth enabled mobile device
15. A method for transferring data to a remoter [sic] internet server by a Bluetooth enabled mobile device

The ’766 Patent Claims Summary
1. A short-range wireless enabled data capture device
4. A system [comprising a data capture device and a cellular phone]
9. A short-range wireless enabled cellular phone
13. A system [comprising a short-range wireless enabled data capture device and a mobile client application for the short-range wireless enabled cellular phone]

The ’121 Patent Claims Summary
1. A short-range wireless enabled data capture device
4. A system [comprising a short-range wireless enabled data capture device and a short-range wireless enabled cellular phone]
7. A short-range wireless enabled cellular phone

9. A short-range wireless enabled data capture device

The ’381 patent Claims Summary
1. A system [comprising a mobile software application for a BT enabled cellular phone and an online data publishing web service]
7. A mobile software application for a Bluetooth enabled cellular phone
12. A mobile software application for a Bluetooth enabled cellular phone

65. The challenged claims also include dependent claims, some of which are also invalid for the reasons set forth in this report.

B. Summary of the Common Disclosure

66. The Challenged Patents share a common specification. The parent patent application was filed on December 12, 2011 as U.S. Patent Application No. 12/333,303, published as U.S. Patent Publication 2009/0172129 (Singh129) on July 2, 2009. The Challenged Patents claim priority to U.S. Provisional Patent Application No. 61/017,202, filed on December 28, 2007. In my analysis here, I considered December 28, 2007 to be the alleged Critical Date. for the Challenged Patents.[1]

[1] The Singh129 Publication is also prior art because of the lack of support for limitations in the claims to the specification.

67. The Singh129 parent publication shares a common specification with the Challenged Patents. For ease of reference, I refer to Singh129 when describing the materials in the specification.

68. Generally, Singh129 relates to pairing a digital data capture device in conjunction with a mobile device for publishing data and multimedia content on a remote server. *See, e.g.*, Singh129, [0003]. As shown below, Singh129's system includes, among other things, digital data capture device 201, Bluetooth (BT) enabled mobile device 202, and publishing service 401. *Id.*, FIGS. 2 & 4. Singh129 FIG. 2 is reproduced below, showing the digital data capture device connected to the Bluetooth enabled mobile device across a Bluetooth connection:

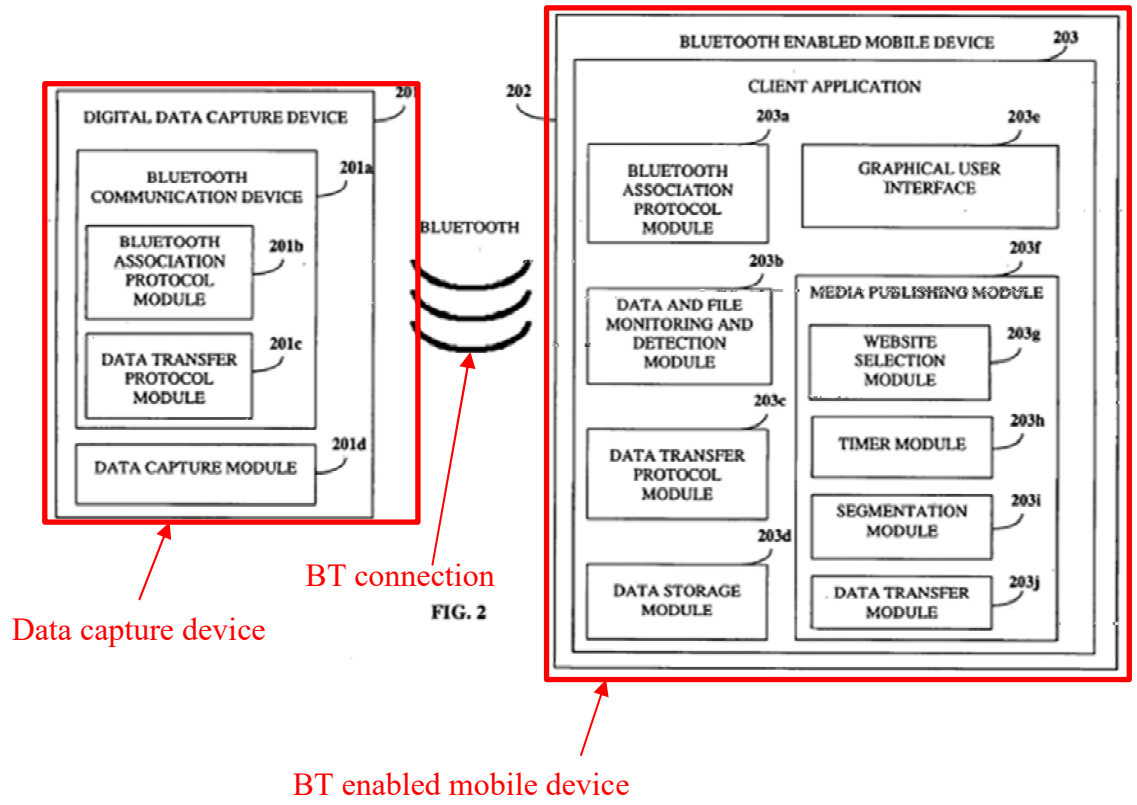


FIG. 2

Singh129, FIG. 2 (annotated).

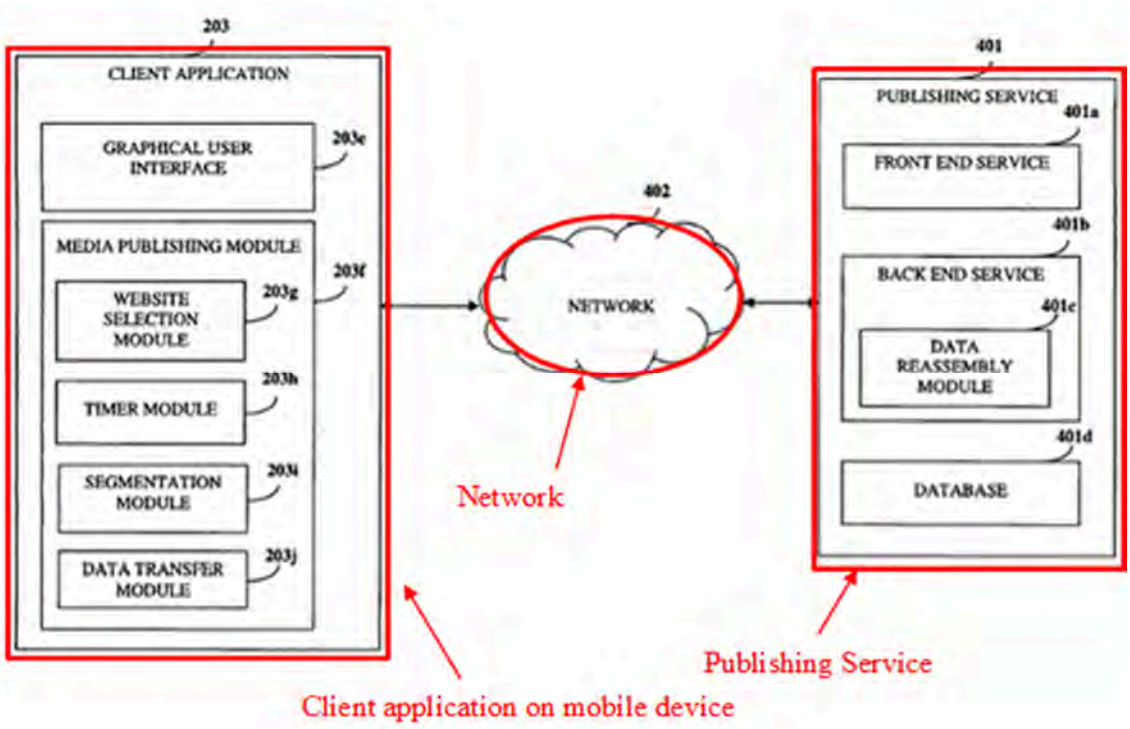
Singh129 describes that the "digital data capture device may, for example, be a digital camera, a video camera, or other digital modular camera systems." Singh, [0009] ("A user may capture data and multimedia content using the digital data capture device."), [0019] ("The digital data capture device 201 may, for example, be a digital camera, a video camera, digital modular camera Systems, or other digital data capturing systems."). According to Singh129, a "Bluetooth enabled mobile device" is also referred to as "mobile device," which may be, for example, "a **ubiquitous** mobile phone." Singh129, [0019], [0046] (emphasis added).

69. The Bluetooth enabled mobile device communicates with the digital data capture device by a Bluetooth connection (which is short-range wireless communication). The "digital data capture device 201 is paired 103 with the mobile device 202 to establish a connection between the digital data capture device 201 and the mobile device 202." Singh129, [0021].

70. The Bluetooth enabled mobile device includes a client application. *See, e.g.*, Singh129, [0008], [0020], [0023]. "The client application 203 on the mobile device 202 comprises a BT association protocol module 203a, a data and file monitoring and detection module 203b, a data transfer protocol module 203c, a data storage module 203d, a graphical user interface (GUI) 203e, and a media publishing module 203f." *Id*., [0033]. As shown in FIG. 4, the system includes "a

client application 203 and a publishing server 401 connected via a network 402." *Id*., [0038] ("The network 402 may, for example, be a wireless network, a cellular network, or the internet 501.").

71. FIG. 4 is illustrated below:



Singh129, FIG. 4 (annotated)

As shown above, client application on the mobile device includes, among other things, a data and file monitoring and detection module 203b, a data transfer protocol module 203c,and a website selection module 203g. Singh129, [0033].

72. Singh129's data and file monitoring and detection module 203b "monitors and detects the capture of the data, the multimedia content, and the files associated with the captured data and the multimedia content." Singh129, [0034].

After data is detected, "the data transfer protocol module 203c of the client application 203 initiates the transfer and download of the captured data, the multimedia content, and the associated files from the digital data capture device 201." *Id*.

73. Singh129 provides some description for how data is detected at the mobile device. Specifically, Singh129 describes a "pull mode" and a "push mode." "In the pull mode, the client application 203 periodically polls the digital data capture device 201 to determine the creation of a new file in the digital data capture device 201." Singh, [0023]. Then, the digital data capture device "**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." *Id*. (emphasis added).

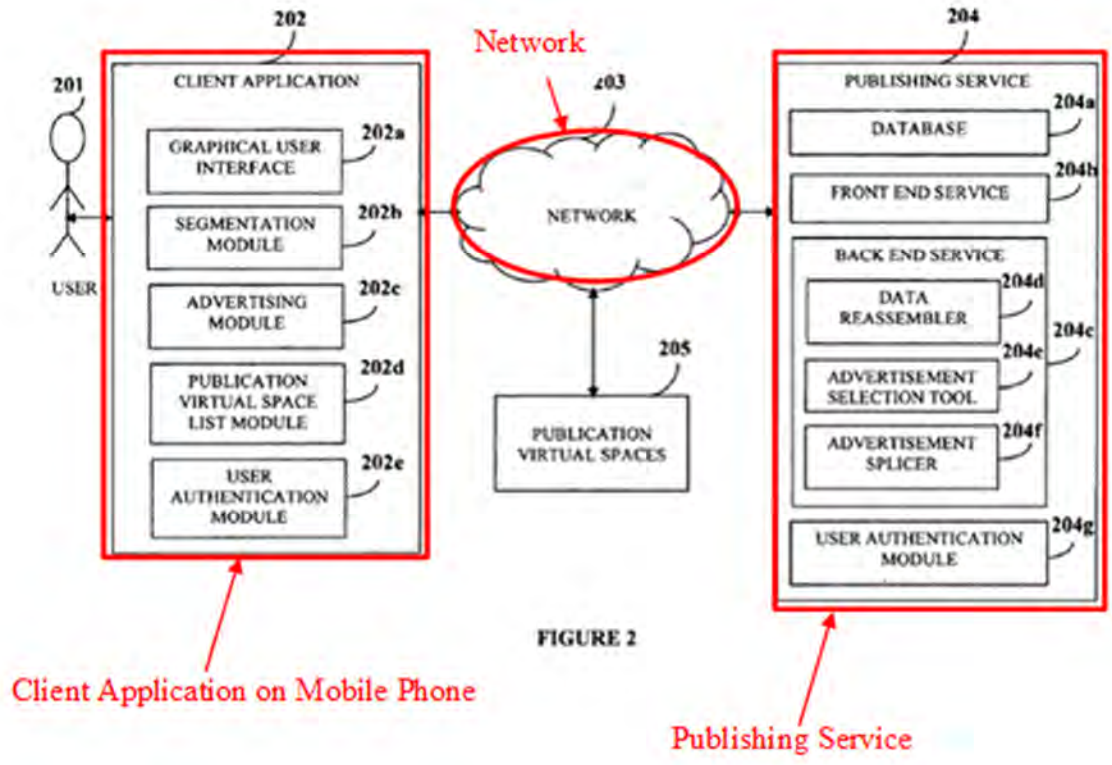
74. In the push mode, Singh129 describes that the digital data capture device "sends a signal to the client application203 on creation of a new file. By implementation of a handshake protocol, the BT communication device 201a [on the digital data capture device] automatically transfers captured data, the multimedia content, and the associated files to the client application203 on the mobile device 202." Singh129, [0025].

75. Noteworthy is that there does not appear to be any teaching or suggestion in Singh129 that the signal to notify the mobile phone of the new file is

included in the new file sent from the digital data capture device to the mobile device.

76. According to Singh129, the website selection module 203g "selects the websites based on settings and user preferences configured by the user on the mobile device 202." *Id*., [0036]; *see also* [0028] ("The user preferences may, for example, comprise the websites selected for publishing the data and the multimedia content."), [0042] ("The user 502 may select websites, for example, Flickr™, Picasa™, YouTube™, eBay®, etc. and store the preferences on the mobile device 202.").

77. The mobile phone transmits the data to the publishing service. "The transferred data and multimedia content is stored in the database 401d of the publishing service 401." Singh129, [0040]. User preferences may be provided to the publishing service through a protocol that synchronizes such information. *See, e.g.*, *id*. According to Singh129, user preferences can include "user preferences of the websites and the timer setting." *Id*. As discussed above, the user preference for websites can include "for example, Flickr™, Picasa™, YouTube™, eBay®, etc. and store the preferences on the mobile device 202." *Id*., [0042]. FIG. 2 of Singh129 shows the client application and the publishing service:



Singh129, FIG. 2 (annotated)

78. Singh129 describes the publishing service as including "websites, for example, Flickr™, Picasa™, YouTube™, eBay®, etc." Singh129, [0042]. Singh129 also includes a blog accessible by a user's work associate as publishing service. *See, e.g.*, *id*., [0045]. In the various claims, the publishing service is referred to as "a remote internet server" in the '030 patent, claim 12 (the term "remote internet server" is not in the specification); "a user data publishing website" in the '766 patent, claim 1; a user data publishing web service in '121 patent, claim 7; and "a remote server" in claim 12 of the '381 patent (the term "remote server" is not in the specification).

79. Note that Singh129 does not describe other user preferences, such as global positioning information. Nor does Singh129 expressly describe sending global positioning information from the mobile device to the publishing service over the cellular network using HTTP. At best, Singh129 describes a "protocol" that is "provided for synchronizing user publishing information between the client application 203 and the publishing service 401" and that the "transport protocol that is used between the client application 203 and the publishing service 401 may be hypertext transfer protocol (HTTP)." Singh129, [0040], [0047].

80. Singh129 patent (at ¶ [0003]) also incorporates by reference U.S. Pat. App. 11/901,802, which published as Signh906 and discloses a "method and system [that] publishes user created multimedia content … on one or more publication virtual spaces, simultaneously." Singh906, Abstract. Notably, Singh906 discloses mobile device client application 202 that includes advertising module 202c. *Id*., Abstract, [0023], FIG. 2. Furthermore, Singh906 discloses publishing service 204 that includes: (i) front end service 204b for publishing the multimedia "according to user preferences," including "authentication credentials" and "global positioning system geographical codes;" (ii) "back end service [204c that] splices targeted advertisements with the multimedia;" and (iii) database 204a, which includes user profiles. *Id*.; *see also* [0028] ("The preferences set by the user 201 [and transferred to the publishing service 204] may be authentication

credentials, transaction identification, list of publication virtual spaces 205, global positioning system geographical codes, area code for the phone number of the mobile device, file format of the user created multimedia content, and compression rate for the user created multimedia content."), [0034] ("The database 204a of the publishing service 204 comprises user profiles, user preferences, advertisement profiles, advertisements, and user created multimedia content.").

81. As explained in Singh906, advertisements may be "displayed to the user 201 on the mobile device after the user 201 has published the user created multimedia content by pressing the post button on the mobile device. The advertising module 202c of the client application 202 displays advertisements targeted to the user 201 on the mobile device." *Id*., [0032]; *see also* [0042], Fig. 3. Similarly, "[t]argeted advertisements based on the user profile may be selected from the database 204a of the publishing service 204 by the advertisement selection tool 204e. The advertisement selection tool 204e of the back end service 204c selects advertisements from the database 204a based on the user profile 201, time, day, and date metrics, advertisement campaigns, preferences of viewers of the published multimedia content, and the type of publication virtual spaces 205. The selected advertisements are then spliced with the multimedia object by the advertisement splicer 204f of the back end service 204c." *Id*., [0036].

C. Summary of Prosecution History

1. '030 patent

82. The '030 patent issued from U.S. Patent Application No. 14/295,353 ("the '353 application"), which was filed on June 4, 2014.

83. On July 8, 2014, the examiner rejected the '353 patent application in an office action. In the office action, the examiner provisionally rejected all the 20 originally filed claims on the ground of non-statutory obviousness-type double patenting as being unpatentable over claims 1-20 of U.S. Patent Application No. 14/295,352. The examiner also rejected all 20 claims under 35 AIA U.S.C. 103(a) over Kennedy (U.S. Patent Publication No. 20043/0157960) in view of Vesuna (U.S. Patent Publication No. 2008/0272185), Hong (U.S. Patent Publication No. 2006/0264176), and Behzad (U.S. Patent Publication No. 2009/0023428).

84. In response to the double patenting rejection, on August 5, 2014, the patent owner filed a terminal disclaimer to overcome the rejection. Furthermore, in response to the 35 AIA U.S.C. 103(a), the patent owner argued that the combination does teach the claimed limitations and amended the claims. The claim amendments were performed in the three independent claims and included limitations directed towards a "cryptographic encryption key", "data signal notification," and amendments in a few dependent claims.

85. On October 3, 2014, the examiner issued a Notice of Allowance for the '353 application. The Notice of allowance included an examiner's amendment

to the claims based on a telephone interview dated September 23, 2014. The examiner's reason for allowance indicated none of the prior art of the record taught or suggested the amended claims.

2. '766 patent

86. The '766 patent issued from U.S. Patent Application No. 15/640,594 ("the '594 application"), which was filed on July 3, 2017. Shortly after filing the patent application, the patent owner agreed to an examiner's amendment to put the claims into condition for allowance. The examiner did not reject the claims using prior art in an office action. The amendments to the claims did not come from originally presented dependent claims.

3. '121 patent

87. The '121 patent issued from U.S. Patent Application No. 16/532,507 ("the '507 application"), which was filed on August 6, 2019. Notably, the examiner rejected the claims as failing to comply with the written description requirement because the specification does not disclose "authentication credentials" and "global positioning system geographical codes" recited in the challenged claims. TTI-1006, 312-313. In response, patent owner relied on the incorporation by reference of the '802 application and reference to Bluetooth. *Id*., 270-.294. The examiner rejected the claims under 112 a second time. *Id*., 245. The applicant amended the claims to address features that were not supported. *Id*.,

184. Despite several rejections under section 112, eventually, the examiner withdrew the rejection, erroneously, in my opinion. *See* Section VII, *infra*.

88. The examiner also rejected the claims in view of prior art. *Id*., 294. The applicant amended the claims to include "wherein the event notification corresponds to the acquired new-data and comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone." *Id*., 259. The applicant also added that the cellular phone stores a user authentication credential, a touch-based GUI, the timer setting, and the use of HTTP to send the user preference (GPS) to the publishing website. *Id*., 7, 21, 184.

4. '381 patent

89. The '381 patent issued from U.S. Patent Application No. 17/542,373 ("the '373 application"), which was filed on December 4, 2021. The claims were first rejected under obviousness-type double patenting, which was overcome by the filing of a terminal disclaimer. TTI-1008, 35, 77.

90. The examiner also rejected the claims as failing to comply with the written description requirement because "display a mobile advertisement inside the mobile software application" and "touch-based advertisement to a user" were not disclosed in the specification. *Id*., 78-80. In response, the Applicant pointed to the Singh906 Application for support. *Id*., 40-47. The examiner withdrew the rejections, which was erroneous in my opinion. *Id*., 10. *See* Section VII, *infra*.

91. The examiner further rejected the claims as obvious in view of prior art. *Id*., 80. The Applicant amended the claims to include "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." *Id*., 26. The examiner subsequently allowed the claims. *Id*., 10.

D. Claim Construction

92. I am informed that all claim terms should be construed according to their ordinary meaning within the context of the Challenged Patents. I do not believe any term requires a formal construction to resolve the issues I discuss in this Declaration. I have not been asked to determine the full scope of any claim term and have not been asked to consider issues of indefiniteness.

93. Nonetheless, I note that for purposes of determining whether to institute IPR2019-00127 regarding related U.S. Pat. No. 9,258,698, the Board "determine[d] that 'cryptographically authenticating identity of the cellular phone,'" which is also recited in various challenged claims here, "encompasses 'authenticating the identity of the cellular phone using some form of security or encryption, including by use of a shared passkey on the digital camera device and the cellular phone.'" *Cannon U.S.A., Inc. v. Cellspin Soft, Inc*., IPR2019-00127, Paper 7, p. 11 (P.T.A.B. April 29, 2019). However, in the Final Written Decision,

the Board found that no construction was required to address the patentability issues. *Id*. at Paper 51, pp. 17-18.

E. Person of Ordinary skill in the art

94. In determining the characteristics of a hypothetical person of ordinary skill in the art ("POSITA") at the time of the claimed invention (using the alleged priority dates), I considered several things, I considered the type of problems at issue in the Challenged Patents. I also considered the sophistication of the technologies involved and the educational background and experience of those actively working in the field at that time. I also considered the level of education that would be necessary to understand the Challenged Patents. Finally, I placed myself back in the relevant period of time, and considered the academics, engineers, and students that I had worked with in the field of consumer electronics.

95. Based on this analysis, I came to the conclusion that the characteristics of a POSITA in the field of art of the Challenged Patents would have had at least a bachelor's degree in electrical engineering, computer engineering, or computer science, and two years of experience in the field consumer electronics, with exposure to digital camera technology and wireless communications. Superior education could compensate for a deficiency in work experience, and *vice-versa*.

VII. PRIORITY ANALYSIS

96. In my opinion, no challenged claim is entitled to an earlier filing date.

97. Each of these patents claims priority, through a series of continuation applications, to a provisional application filed on December 28, 2007. The challenged claims, however, were each introduced many years later.

98. Patent Owner first introduced the challenged claims of the ’766 patent in an application filed on July 3, 2017.

99. Patent Owner first introduced the challenged claims of the ’121 patent in an amendment filed on October 16, 2020.

100. Patent Owner first introduced the challenged claims of the ’381 patent in an amendment filed on February 9, 2023.

101. Patent owner first introduced the challenged claims of the ’030 patent in amendments filed on August 5, 2014 and October 9, 2014.

A. The challenged claims of the ’766, ’121, and ’381 patents mix and match features from different systems

102. The challenged claims of the ’766, ’121, and ’381 patents combine features from client application 203, which is disclosed in the priority applications themselves (Singh129 is representative), with features from a distinct client application (“client application 202”), which is disclosed in U.S. Pat. App. No. 11/901,802 (“the ’802 application)—an unrelated application that is incorporated by reference into each priority application. *Id*. The ’802 application published as U.S. Pat. App. Pub. No. 2008/0103906 (“Singh906”).

103. Client applications 202 and 203 have different numbers because they are different software programs that address different perceived problems in the prior art. Client application 202, for example, addresses the purported "unmet need for a method and system to create and publish multimedia content online using a ***single*** device." TTI-1010 (Singh906), [0003] (emphasis added). In contrast, client application 203 addresses the purported "need for a method and system to utilize a [separate] digital capture device ***in conjunction with*** a mobile device for automatically detecting capture of data and multimedia content, transferring the captured data and multimedia content to the mobile device, and publishing the data and multimedia content on one or more websites automatically." TTI-1010 (Singh129), [0005] (emphasis added). Moreover, the two applications are clearly directed toward dramatically different users—*i.e.*, those that create content with their phones (client application 202) and those that create content with a separate digital capture device (client application 203) while using a phone merely as an internet connection.

104. There are numerous differences between the two applications. For example, unlike Singh906's client application 202, Singh129's client application 203 does not: (i) provide targeted advertising to the user; (ii) provide to a remote server authentication credentials, transaction identifications, a list of publication virtual spaces, global positioning system geographical codes, area codes for the

phone numbers of the mobile device, file formats of the user created multimedia content, or compression rates of multimedia content; (iii) allow the user to identify publication virtual spaces that include meta-destinations; (iv) allow the user to identify other users of any system as publication destinations; (v) allow the user to identify arbitrary emails and phone numbers as a destination; (vi) allow the user capture multimedia using the mobile device itself; (vii) allow the user to change the quality of the multimedia; or (viii) provide buttons in a GUI to control the playback of a recorded message. In fact, instead of allowing the user to review and delete recorded media on their phone, as is done with Singh906's client application 202, Singh129's client application 203 automatically publishes images to one or more websites. Furthermore, Singh129 expressly teach that using client application 203 to "shar[e] information over electronic mail (emails)," as is done with Singh906's client application 202, "may be inconvenient." TTI-1009 (Singh129), [0045].

105. Similarly, unlike Singh129's client application 203, Singh906's client application 202 does not detect, receive, store, or transfer data acquired in a Bluetooth enabled data capture device and it does not include a timer module for setting the time to automatically publish multimedia content. Moreover, there is no indication in Singh906 that the mobile device on which client application 202 runs is a Bluetooth enabled cellular phone and thus no indication that client

application 202 would have even been capable of detecting or receiving data acquired in a Bluetooth enabled data capture device, much less in the specific way claimed in the ’766, ’121, and ’381 patents. In any event, receiving data from a separate data capture device would have been inconsistent with the stated purpose of client application 202 to create and publish multimedia content using a single device.

106. Nonetheless, claim 1 of the ’766 patent recites a mobile client application that (1) obtains data from a “short-range wireless enabled data capture device,” and (b) “use[s] HTTP to upload the received new-data along with user information to a user data publishing website over a cellular 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.” Each of the other independent claims (4, 9, and 13) include essentially the same limitations. Notably, during prosecution of U.S. App. No. 14/503,401, to which the ’766 patent claims priority, the applicants confirmed that this “user information is to make sure only [the user] can post to [their website (e.g., blog)], and [that] the remote website will use that [user information] to check/authorize the uploaded content for that particular … user.” TTI-1033, 182-243.

107. Similarly, claim 1 of the ’121 patent recites the following limitations:

"wherein the user preference comprises global positioning system information;" "wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone stores a user authentication credential in the memory device of the cryptographically authenticated short-range wireless enabled cellular phone;" and "use HTTP to upload … the user authentication credential to a user data publishing website over a cellular data network." Essentially the same limitations are included in each of the other independent claims.

108. However, there is no description in the specification of the priority applications of a client application using HTTP to upload such user information to a user data publishing website or using such user information to publish the new data for private consumption. Indeed, the only examples in the specification of the priority applications of information provided by the user are: (1) websites selected for publishing; and (2) timer and action settings. I understand that Patent Owner may argue that providing the claimed "user information" in the '766 patent is inherent in the "blog post" example of the priority documents. *See*, *e.g.*, TTI-1009, [0045]. However, I disagree with that argument because it is not disclosed explicitly. As described, "Jane's private blog" is accessible by various individuals, but the criteria and mechanisms for access are not specified. For example, a shared token may be used, which would not uniquely identify an individual. The

information sent from the client application may, for example, be based on an Internet "session" (or some other state or event), which may entail the sending of a session (or state or event) identifier, but not "user information." In addition, even if user information were sent from the client application, that information may be sent to an authentication server or other backend server before being routed to the user data publishing website over the backbone (non-cellular) Internet, rather than to the "user data publishing website over the cellular data network." A skilled artisan would not understand the general disclosure of the priority documents to disclose the claimed system explicitly.

109. Not surprisingly, during prosecution of the application that issued as the '121 patent, the examiner correctly noted that the specification "fails to sufficiently point out or describe ... ***wherein the user preferences comprise authentication credentials and global positioning information***." TTI-1006, 310 (emphasis original); *see also* TTI-1006, 241 (further noting that "the applicant fails to sufficiently point out or describe … ***wherein the user preferences comprise authentication credentials and use HTTP to send global positioning system information to the user data publishing website over the cellular data network***") (emphasis original). As support for these limitations, Patent Owner directed the examiner only to pages 5, 7, 9 and Figures 2 and 4 of U.S. Pat. App. No. 11/901,802, which published as Singh906 and is incorporated by referenced into

the priority applications. TTI-1006, 271, 194.

110. These citations, however, refer only to Singh906's client application 202, which does not include at least the following elements of the systems claimed in the '766 and '121 patents: (1) a short-range wireless enabled data capture device comprising; (2) a short-range wireless communication device configured to; (a) establish a paired wireless connection with a cellular phone, wherein establishing the connection comprises; (b) cryptographically authenticate the identity of the phone; (c) acquire new-data after establishing the paired connection; (d) store the new-data; and (e) send an event notification and the new-data to the phone automatically; and (3) a single mobile client application for the phone that is configured to (a) listen for and process the event notification; (b) store new-data from a separate data capture device; or (c) use HTTP to upload the new-data based on timer settings. Moreover, Singh906's client application 202 does not use HTTP to upload/send to a user data publishing website any authentication credentials or global positioning system information as required by the challenged claims. Instead, Singh906's client application 202 uploads/sends this information to publishing service 204, which is not a user data publishing website.

111. Like the '766 and '121 patents, the challenged claims of the '381 patent recite the following limitations: "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;" and "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." As explained above, however, this feature is described only in the context of Singh906's client application 202.

112. The challenged claims of the '381 patent also recite the following limitation: "display a mobile advertisement inside the mobile software application."

113. However, during prosecution of the '373 application, which issued as the '381 patent, the examiner noted that the specification "fails to sufficiently point out or describe ***display a mobile advertisement inside the mobile software application*** & ***touch-based advertisements targeted to a user***." TTI-1008, 78-80 (emphasis original). Patent Owner disagreed and, as support for this element, Patent Owner directed the examiner only to Figure 3 and paragraph [0021] of Singh906—the publication of U.S. Pat. App. No. 11/901,802, which is incorporated by referenced into the '373 application. *Id*., 40-47.

114. Again, however, these citations refer only to Singh906's client application 202, which does not perform at least the following functions of the systems claimed in the '381 patent: (1) detect and receive new-data acquired in a

Bluetooth enabled data capture device after establishing a paired Bluetooth connection and cryptographically authenticating an identity of a cellular phone; (2) either listen for an event notification sent from a data capture device over an established paired Bluetooth connection or poll a Bluetooth enabled data capture device for new data; (3) receive from a data capture device either an event notification or acquired new-data; (4) store received new-data in a memory of a cellular phone; and (5) use HTTP to transfer received new-data to a remote server over a cellular data network. Also note that despite citing to Singh906 generally, the Patent Owner did not point to specific disclosure in Singh906 that shows the touch-based advertisements. TTI-1008, 41 (showing ads on a phone but not specifying touch-based ads).

115. Although not identified by the examiner of the '373 application, for each challenged claim, the specification also fails to describe a system that includes the following elements combined with the other elements recited claim elements:

- "wherein the database [of the online data publishing web service] stores a user profile;"
- "a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected

advertisements to the mobile software application."

For claim 1 of the '381 patent, the specification further fails to describe a system that includes each recited claim element in combination with:

- "a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application;"
- "a database, wherein the database stores a user profile;"
- "a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application;"
- "said online data publishing web service configured to receive the new-data and the user authentication credential from the Bluetooth enabled cellular phone via the Hypertext Transfer Protocol;" and
- "said online data publishing web service configured to process the received user authentication credential and the new-data."

Like the elements identified by the examiner, these claim elements are described only in Singh906 in connection with a system that is significantly different from the system described in the priority applications and there is no disclosure of using these elements from client application 202 with client application 203.

116. Furthermore, there is no disclosure in the priority applications directing a person of ordinary skill in the art to use any of Singh906's features in client application 203, much less use the specific features recited in the challenged claims. Although the priority applications incorporate Singh906 by reference (along with numerous related applications), the priority applications themselves do not identify any features disclosed in Singh906. In fact, Singh906 is not mentioned or otherwise referenced in the specification. Likewise, the '802 application is missing most of the limitations of the challenged claims, such as the data capture device, signal to notify, short-range wireless communications, paired wireless connection with cryptographic authentication, and touch-based advertisements, others.

117. Finally, I have been informed that the disclosures in the '802 application identified by Patent owner as support for various claim elements are "essential material" because they were identified by Patent Owner as necessary to satisfy the written description requirement. However, I have also been informed that essential material may only be incorporated by reference "by way of . . . a U.S. patent or U.S. patent application publication," and **not** by incorporation of an unpublished application. The '802 application is not a U.S. patent or a U.S. Patent application publication. Accordingly, I have been informed that the challenged patents do not incorporate by reference the essential material identified by Patent

Owner as support for the challenged claims and that the information disclosed in the ’802 application cannot be used to show written description support for the challenged claims in the priority applications.

118. Thus, in my opinion, no challenged claim of the ’766, ’121, and ’381 patents can claim priority to an earlier application. Accordingly, Singh129 and Singh906 are prior art to the ’766, ’121, and ’381 patents.

B. The ’030 patent does not describe elements of the claimed inventions

119. No priority application for the ’030 patent describes any of the following elements of the challenged claims:

- “performing at a Bluetooth enabled data capture device … encrypting, using cryptographic encryption key, the new data [object] acquired in the Bluetooth enabled data capture device; and transferring the encrypted data [object] from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection … wherein the Bluetooth enabled mobile device is configured to receive the encrypted data [object] and obtain the new data [and the data signal notification] from the encrypted data using cryptographic encryption key” (claims 1, 6)
- “receiving, by the Bluetooth enabled mobile device, encrypted data [object] corresponding to the new data [object] over the established

Bluetooth paired secure wireless connection and obtaining new data[, data associated with new data and time-stamp] from the received encrypted data [object] using cryptographic encryption key" (claims 12 and 15)

- "sending a message to the Bluetooth enabled mobile device / [receiving a message from the Bluetooth enabled data capture device], corresponding to supported data capability of the Bluetooth enabled data capture device" (claims 1 and 12)
- "wherein new data object comprises of new data, data associated with new data and time-stamp, and wherein the time-stamp corresponds to a time when new data was acquired" (claim 15)

120. A POSITA reading the priority applications would not immediately discern these limitations, nor would a POSITA consider them to be necessarily disclosed in the priority application. Indeed, the priority applications contain no written description of a data capture device encrypting acquired data or transferring encrypted data to a mobile device of a Bluetooth connection and thus no written description of a mobile device receiving/obtaining encrypted data from the data capture device. Rather, the priority applications merely describe a Bluetooth pairing process and transferring data over a Bluetooth connection. Notably, data encryption was an optional feature of Bluetooth at the time of the claimed

invention. TTI-1019 (Bluetooth), 868. Similarly, no priority application contains a written description of sending/receiving a message corresponding to supported data capability of the Bluetooth enabled data capture device. And no priority application contains a written description of a new data objection comprising a time-stamp corresponding to a time when new data was acquired. Thus, in my opinion, no challenged claim of the '030 patent can claim priority to an earlier application. Accordingly, Singh129 is prior art to the '030 patent.

VIII. SUMMARY OF THE PRIOR ART

121. In my opinion, the prior art discussed below teaches the same concepts that the Challenged Patents hold out as the alleged invention—wirelessly connecting a digital camera to a mobile device for publishing content captured by the digital camera on a remote server. This was well known in the prior art prior to December 28, 2007, along with minor aspects of the challenged claims, like using non-volatile storage, image upload via HTTP, and cryptographic authentication between wireless devices.

A. Hiroishi

122. Hiroishi is a Japanese patent application published on February 28, 2003 and assigned to Fuji Photo Film Co., Ltd. Hiroishi, Face. I understand that Hiroishi qualifies as prior art under pre-AIA 35 U.S.C. § 102(b). *Id*. I understand that TTI-1011 is the original Japanese language publication for Hiroishi, TTI-1011

is a certified English translation of Hiroishi, and TTI-1012 is an affidavit certifying the translation of Hiroishi.

123. Hiroishi teaches a system that allows users to use a mobile phone to control a digital camera remotely. Hiroishi, Abstract, [0043] ("As shown in the drawing, the photographing system 10 according to this embodiment is a system wherein various keys provided to the mobile phone 40 are used to remotely operate the digital camera 50 by transmitting various instruction information from the mobile phone 40 to the digital camera 50."). In addition, Hiroishi discloses a "two-way wireless communication" using Bluetooth. *Id*. [0066] ("The photographing system 10 according to this embodiment is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth.").

124. In one embodiment, a release instruction is issued by the mobile device, which in turn causes the camera to acquire and store new photographs. *Id*. [0078] ("In Step 114, a determination is made as to whether the instruction information received in Step 104 is the release instruction information; if yes, the process goes to Step 116, a predetermined image processing is performed to the digital image data input from A/D converter 53, the image recording processing for storing it in the photographed image data storage area (not shown) of SDRAM 55A is subsequently performed, and the process returns to Step 104."). Once at "step

104," the mobile device may then instruct the digital camera to transmit the stored image data to the mobile device. *Id*. [0084]. The camera may also transmit a thumbnail of the image to the mobile device. *Id*. [0081].

125. 76. Once received, the mobile device may then upload it to another computing device. *Id*. [0044] ("When the digital camera 50 receives from the mobile phone 40 the instruction information for the purpose of transmitting the image information obtained by photographing, the photographing system 10 transmits the image information to the mobile phone 40, and the mobile phone 40 forwards the image information received from the digital camera 50 to a terminal device.").

B. Takahashi

126. Takahashi is a Japanese patent application published on October 27, 2005. Takahashi, Face. I understand that Takahashi qualifies as prior art under pre-AIA 35 U.S.C. § 102(b). *Id*. I also understand that TTI-1014 is the original Japanese language publication for Takahashi, TTI-1016 is a certified English translation of Takahashi, and TTI-1015 is an affidavit certifying the translation of Takahashi.

127. Takahashi teaches the use of mobile devices for uploading image data to remote servers immediately after capturing using HTTP. *See, e.g.*, Takahashi, [0020]. Takahashi, Abstract, [0049]. A user ID is also uploaded along with the

image data to identify the user. *Id.* [0066] ("In the mobile phone 1, when an image data is transmitted to the image storage server 4, the user on the image storage server 4 side is specified by including the user ID in the file name of image data."). Once received, the image storage server processes (e.g., resizes) the image prior to publishing the image to a webpage. *Id*. [0052] ("The image storage server 4 performs a resize process of an image in order to publish the image on a web page.").

128. Takahashi teaches a system that allows a mobile device to use HTTP to upload image data to a remote server that processes the received image data in order to publish and share it on a user media publishing website. Takahashi, [0062] ("The image publishing processing unit 23 performs processing in publishing the image data from the mobile phone 1 to a web page."), Abstract ("a mobile telephone 1… sends the data to an image storage server 4 as an HTTP request"), [0052] ("The image storage server 4 performs a resize process of an image in order to publish the image on a web page."), [0037] ("the image data can be shared by publishing the stored image data"). The user can choose what images to publish and share. Id. [0063] ("an image selection screen for allowing the user of the mobile phone 1 to select the publishable image data from among the stored image data").

129. Takahashi further teaches that the uploaded information includes the

image data, along with a filename that identifies user information including a user ID. Id. [0066] ("In the mobile phone 1, when an image data is transmitted to the image storage server 4, the user on the image storage server 4 side is specified by including the user ID in the file name of image data.").

C. Kahn

130. U.S. Patent Publication 2004/0004737 to Kahn at al. ("Kahn"), titled, "Imaging System Providing Automated Fulfillment of Image Photofinishing Based on Location," was filed on July 2, 2002 and published on January 8, 2004.

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

132. In addition, Kahn teaches that the host device (i.e., the cellular phone) "communicates with an online Web-based image management server 330" using, for example, "HTTP protocol." Kahn, [0056].

D. Endsley

133. U.S. Patent Publication No. 2006/0139474 to Endsley is titled "System and Camera for Transferring Digital Images to a Service Provider." Endsley was filed on February 16, 2006 and was published on June 29, 2006. Generally, Endsley is about "a digital camera system which allows for automatically transferring digital image data." Endsley, [0009].

134. In Endsley, a digital camera can be used to capture images. *See, e.g.*, Endsley, [0028]. Endsley notes that in prior art systems, cameras or camera memory would need to be taken physically into a print shop or photofinisher to produce prints. *See, e.g.*, Endsley, [0004]-[0007]. Endsley teaches transferring the digital images to a remotely located site using a communications network. *See, e.g.*, Endsley, [0009], [0044].

E. Feinberg

135. U.S. Patent Publication no. 2007/0073937 to Feinberg is titled, "Content-Aware Digital Media Storage Device and Methods of Using the Same." Feinberg was filed on August 29, 2006 and published on March 29, 2007. Feinberg is about storage media for digital media devices such as cameras, audio/video recorders/players, and the like, and, more particularly, to such storage media as incorporate peripheral devices for transferring digital media stored therein via wireless communication links or otherwise processing said media."

Feinberg, [0002]. Specifically, it discusses digital cameras with wireless network connectivity, compatible with IEEE 802.11 standards, enabling image data transfer to computers or printers. Id., [0002], [0005]. Furthermore, Feinberg discloses uploading images to internet-based storage via mobile phones. Id., [0049].

136. Feinberg describes various metadata that can be associated with or included with images captured by a digital camera. For example, Feinberg mentions that "digital cameras typically associate non-visual information (so-called metadata) with images (usually at or about the time the image is recorded)." *See, e.g.*, *id.*, [0076]. According to Feinberg, metadata information can include "the date and time the image was captured, the camera settings used to take the image and user-customized comments." *Id*. In addition, Feinberg states that thumbnails can also be created. *See, e.g.*, *id*., [0091]. For example, thumbnail images (e.g., having 160x120 pixel resolution) are typically embedded into the full resolution image file header." *Id*.

IX. OVERVIEW OF THE GROUNDS

137. The following summarize the invalidity grounds:

The '030 Patent		
Ground	Claims	Prior Art
Ground 1A	1-2, 4-7, 9-18	Hiroishi, Takahashi, Bluetooth

Ground 1B	1-2, 4-7, 9-18	Hiroishi, Kahn, Bluetooth
Ground 2A	1-2, 4-7, 9-14	Singh129, Singh906, Bluetooth
Ground 2B	1-2, 4-7, 9-14	Singh129, Singh906, Bluetooth, Takahashi

The ’766 Patent		
Ground	Claims	Prior Art
Ground 1	1-15	Singh129, Singh906
Ground 2A	1-15	Kahn, Bluetooth
Ground 2B	1-15	Kahn, Feinberg, Bluetooth

The ’121 patent		
Ground	Claims	Prior Art
Ground 1	1-10	Hiroishi, Kahn, Endsley, Bluetooth
Ground 2	1-10	Singh129, Singh906

The ’381 Patent		
Ground	Claims	Prior Art
Ground 1	1-16	Hiroishi, Kahn, Bluetooth
Ground 2	1-16	Singh129, Singh906

X. INVALIDITY ANALYSIS OF THE '030 PATENT

A. Ground 1A – Hiroishi in combination with Takahashi and Bluetooth V2.1 Renders Claims 1-2, 4-7, 9-18 Invalid

138. Hiroishi teaches a photograph system that includes a cellular phone that connects to a camera via a Bluetooth connection. The cellular phone can control the camera to capture images, store images, and transmit images to the cellular phone. The cellular phone can then transmit images to a remote computer destination by a cellular network connection via the Internet. In the combination, the mobile phone of Hiroishi is configured to apply an action setting that includes an HTTP method to the received images from the camera, in a manner similar to what was suggested by Takahashi. Also in the combination, Hiroishi sends a user identifier with the transmission of the images, like in image file name taught by Takahashi. In the combination, Hiroishi sends a time-stamp of when the image or images were taken, in a manner similar to what was suggested by Takahashi.

139. In addition, in the combination, the Bluetooth-enabled camera of Hiroishi encrypts the image data transmitted to Bluetooth-enabled cellular phone over the Bluetooth connection using an encryption technique consistent with the teachings of the Bluetooth 2.1 Core Specification. In the combination, the camera of Hiroishi provides a message corresponding to supported device capabilities to the mobile phone (e.g., after a Bluetooth connection has been established), as

described by the Bluetooth Core Specification V2.1.

1. The Predictable Combination of Hiroishi, Takahashi, and Bluetooth Core Specification 2.1

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

141. In addition, in the combination, based on Hiroishi, the Bluetooth-enabled camera encrypts the image data transmitted to Bluetooth-enabled cellular phone over the Bluetooth connection using an encryption technique consistent with the teachings of the Bluetooth 2.1 Core Specification. Also similar to Hiroishi and as further described by the Bluetooth Core Specification V2.1, in the combination, the camera provides a message corresponding to supported device capabilities to

the mobile phone (e.g., after a Bluetooth connection has been established).

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

The combination of Hiroishi and Takahashi

143. First, both Hiroishi and Takahashi are analogous art to the claimed invention. Both references are from the same field of endeavor as the claimed invention: wireless image transfer from one electronic device to another. Hiroishi teaches techniques for enabling a mobile device to control a digital camera and transfer image files between and instructions between the two devices. Hiroishi, Abstract, [0066]. Takahashi is directed to wirelessly transferring image files from a mobile device to a publishing website over the Internet with an action setting. Takahashi, Abstract, [0049], [0051], [0054] (describing the action setting associated with dividing the images for transmission using HTTP).

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

cellular phone to a website using HTTP. *See, e.g.*, Takahashi, [0049].

145. Second, a POSITA would have been motivated to use Takahashi's upload technique to publish image data received at the mobile device of Hiroishi. At the time of the alleged Critical Date, photo-sharing websites and personal blogs had become ubiquitous. *See, e.g.*, TTI-1020, 3:25-49, 4:47-67; TTI-1021, 5:49-56 (describing use HTTP to send images from the phone to the server). Websites like FLICKR, PHOTOBUCKET, and PICASA allowed users to publish photographs and share them with friends, colleagues, and internet users. *See, e.g.*, TTI-1018, 5:25-28; TTI-1022, [0032].

146. Cellular phones had also become ubiquitous. The original iPhone was released six months before the provisional filing date of the '030 patent (the iPhone was released on June 29, 2007), and years before that companies like Blackberry, Motorola, and Nokia had developed cellular phones that allowed users to transfer image data over the Internet. *See e.g.*, Hiroishi, [0015], [0047], FIG. 2. The '030 patent even refers to mobile phones as "ubiquitous." '030 patent, 9:46-47 ("The mobile device 202 may, for example, be a **ubiquitous mobile phone**.") (emphasis added). Takahashi recognizes both of these trends and teaches an efficient and predictable technique for uploading image data from a mobile device to a publishing website. *See, e.g.*, Takahashi, Abstract.

147. The teachings of Takahashi would have provided straightforward

benefit to the user of the mobile device in Hiroishi: predictable upload of image files and an action setting using an existing HTTP connection between the mobile device and a publishing server. Hiroishi already teaches the desire to transfer image data from a digital camera to a mobile device to a terminal device. Hiroishi, [0044]. Takahashi would have furthered this purpose by allowing the user to share image data over the Internet in a straight-forward and well-known way.

148. Third, a POSITA would have been motivated, and found it obvious, to include user identifier that uniquely identifies a particular user of the Internet service. Hiroishi already teaches that the email address of the destination terminal is used to send images to the destination terminal. Hiroishi, [0110]. Because the 030 claims do not require that the user identifier uniquely identifies the operator of the mobile phone, Hiroishi alone would invalidate this feature. If necessary, 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. *See, e.g.*, Takahashi, [0055]. "In the mobile phone 1, when an image data is transmitted to the image storage server 4, the user on the image storage server 4 side is specified by including the user ID in the file name of image data." Takahashi, [0066]. This way, a POSITA would recognize the advantage of being able to uniquely identify the owner of the images, e.g., by the file name, as taught by Takahashi. In the example scenario of Hiroishi's print shop, the print shop worker can quickly and

easily identify the owner of the images by the file name, and can validate the owner when providing the printed images. *See also* TTI-1011, [0110]-[0113].

149. A POSITA would have found it obvious to modify Hiroishi to include a time-stamp with the images, in a manner similar to that suggested by Takahashi. A POSITA would have recognized that including a date and time of when the images were captured would provide additional contextual information to the images. In addition, adding a time-stamp to the image file name would also uniquely identify the image file so that similar images can be quickly distinguished from each other. Using the time-stamp in the image file name also allows the images to be sorted and organized in an online album. A POSITA would have found it obvious to modify the image file names of Hiroishi for at least these reasons. Adding a time-stamp to the file names of the images would have been well within the skill of a POSITA at the time. As described by Takahashi, the time and date (to the second) could have been derived from an internal clock. *See, e.g.,* Takahashi, [0070], [0084]. Even though as Takahashi's internal clock is in the phone and transmitted to the camera, a POSITA would understand that a more accurate time stamp would be at the camera when the camera takes the picture, so it would have been obvious to add time stamp at the camera. It was also typical as of the alleged Critical Date to have a picture's time stamp added by digital camera. Kahn, [0008], [0060].

150. I note that the ’030 patent specification does not provide written description support for the camera (or other data capture device) sending a time-stamp to the mobile phone. At best, the ’030 patent describes the “segmentation module 203i [at the mobile phone] generates segment identifiers and tags the data segments with the segment identifiers. The segment identifiers may, for example, be one or more of transaction identifiers, sequence numbers, and timestamps.” ’030 patent, 7:55-59. While I believe that the transmission of a time-stamp from the camera to the phone with the images would have been an obvious modification to Hiroishi, the ’030 patent does not provide any written description support for doing so.

151. Note that the PTAB has already accepted that it would have been obvious to combine Hiroishi with Takahashi, for at least some of the reasons articulated above. *See, e.g.*, Petition for IPR, IPR2019-00127, at 51-53, Institution Decision, IPR2019-00127, at 30-34.

The combination of Hiroishi-Takahashi and Bluetooth

152. A POSITA would have also found it obvious that the camera of Hiroishi would have provided a message corresponding to the supported data capability of the camera to the mobile phone upon establishment of the Bluetooth connection, in a manner consistent with the protocols described in the Bluetooth Core Specification. *See, e.g.*, Bluetooth Core Specification V2.1, 441 (4.3.4

Supported Features), 384 (3.2 Feature Definitions). A POSITA would have recognized the benefits of indicating the camera's supported data capability. For example, the mobile phone, as the "master" of the Bluetooth connection, would have used the supported data capability of the camera to configure the Bluetooth communication channel, so that communications between the camera and the mobile phone across the Bluetooth channel would be efficient and resource friendly.

153. In addition, the reporting by the camera of supported data capability includes whether the camera supports encryption. *See, e.g.*, Bluetooth Core Specification V2.1, 384-389. A POSITA would have recognized the benefits of reporting whether the camera supported data encryption so that the mobile phone could enable an encryption protocol to protect the data from malicious attacks, eavesdropping, or other intrusion. An example of supported features in Bluetooth are summarized in Section 3.2 of the Bluetooth specification. TI-1019, 384-389.

154. An example of supported features in Bluetooth are summarized in Section 3.2 of the Bluetooth specification. TI-1019, 384-389.:

Feature	Definition
3 slot packets	This feature indicates whether the device supports the transmission and reception of both DM3 and DH3 packets for the transport of traffic on the ACL-U logical link.

5 slot packets	This feature indicates whether the device supports the transmission and reception of both DM5 and DH5 packets for the transport of traffic on the ACL-U logical link.
AFH capable slave	This feature indicates whether the device is able to support the Adaptive Frequency Hopping mechanism as a slave as defined in Baseband Specification, Section 2.3, on page 70 using the LMP sequences defined in Section 4.1.4 on page 227.
Encryption	This feature shall be supported. This feature indicates whether the device supports the encryption of packet contents using the sequence defined in Section 4.2.5 on page 248.
Enhanced Data Rate ACL 2 Mbps mode	This feature indicates whether the device supports the transmission and reception of 2-DH1 packets for the transport of traffic on the ACL-U logical link.
Enhanced Data Rate ACL 3 Mbps mode	This feature indicates whether the device supports the transmission and reception of 3-DH1 packets for the transport of traffic on the ACL-U logical link. This feature bit shall only be set if the “Enhanced Data Rate ACL 2 Mbps mode” feature bit is set.
3-slot Enhanced Data Rate ACL packets	This feature indicates whether the device supports the transmission and reception of three-slot Enhanced Data Rate packets on the ACLU logical link. This feature bit shall only be set if the “Enhanced Data Rate ACL 2 Mbps mode” feature bit is set.
5-slot Enhanced Data Rate ACL packets	This feature indicates whether the device supports the transmission and reception of 5-slot Enhanced Data Rate packets for the transport of traffic on the ACL-U logical link. This feature bit shall only be set if the “Enhanced Data Rate ACL 2 Mbps mode” feature bit is set.

Example Features Definition, Bluetooth Core Specification V2.1, 384-388.

155. I note that the limitation for transmitting a message corresponding to the supported data capability is not supported by the '030 patent specification. To the extent that the patent owner argues that transmitting a message from the camera to the mobile phone corresponding to the supported data capability is mandatory by the Bluetooth Core Specification, TTI-1036, 31, the claim limitation is invalid based on the combination of Hiroishi, which teaches the use of a Bluetooth connection for transmitting images from the camera to the mobile phone. *See, e.g.*, Hiroishi, [0066]-[0067]; TTI-1019, 133-135.

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

157. A POSITA would have recognized the benefits of implementing encryption of data in the Hiroishi-Takahashi combination. For example, a POSITA would have recognized that encrypting the data protected the data from being intercepted and decrypted by a malicious attacker or other unauthorized

accesses. A POSITA implementing Bluetooth encryption would have had a reasonable expectation of success encrypting data. The Bluetooth Core Specification 2.1 also teaches how to activate encryption between two Bluetooth devices (*see, e.g.*, *id*., 884 ("Set Connection Encryption")), as well as how to perform encryption to protect the payload (*see, e.g.*, *id*., 919 ("1 ENCRYPTION SAMPLE DATA")). For example, the Bluetooth Core Specification 2.1 suggests a "Massey and Rueppel method." TTI-1019, 1038, 1040-1047 (providing examples of how encryption can be implemented).

Reasonable expectation of success

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

159. Similarly, a POSITA implementing Bluetooth encryption in the combination would have had a reasonable expectation of success. The Bluetooth Core Specification 2.1 also teaches how to activate encryption between two Bluetooth devices (see, e.g., TTI-1019, 884 ("Set Connection Encryption")), as well as how to perform encryption to protect the payload. TTI-1019, 919 ("1

ENCRYPTION SAMPLE DATA"). For example, the Bluetooth Core Specification 2.1 suggests a "Massey and Reuppel method." *Id*., 1038, 1040-1047 (providing examples of how encryption can be implemented).

2. Analysis

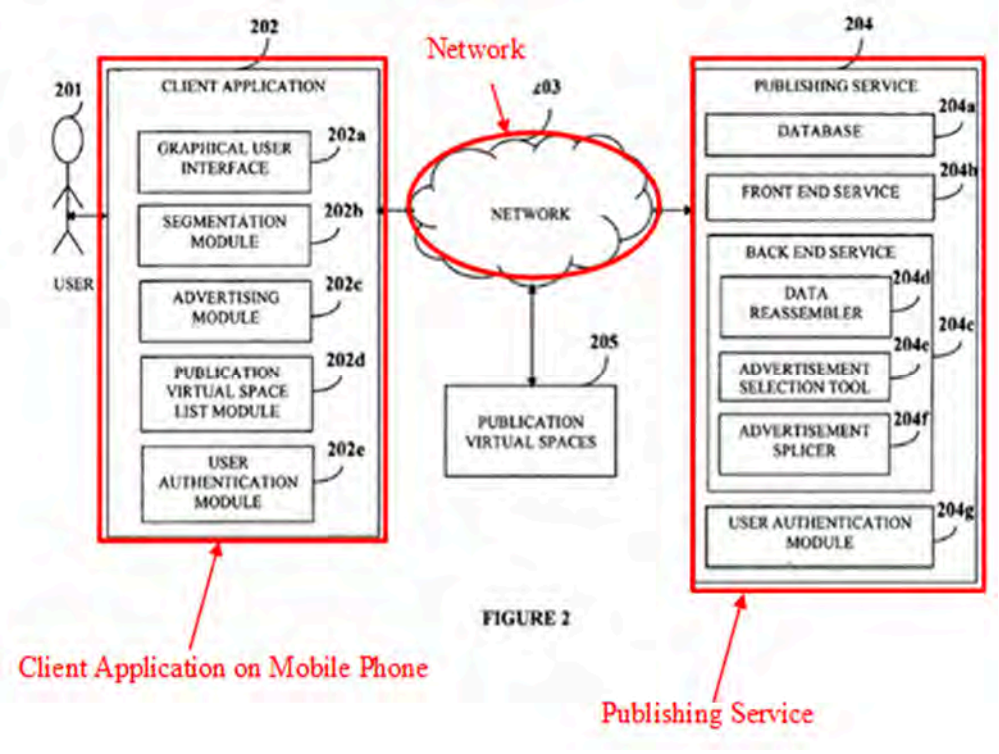
Claim 12

[12.P]A method for transferring data to a remote internet server by a Bluetooth enabled mobile device comprising:

160. To the extent the preamble is limiting, the Hiroishi-Takahashi combination renders obvious element [12.P]. The Hiroishi-Takahashi system performs a method for transferring data (e.g., images taken by Hiroishi's digital camera 50) to a remote internet server (e.g., a terminal device of a print shop) by a Bluetooth enabled mobile device (Hiroishi's cellular phone 40). *See, e.g*., Hiroishi, [0042], [0061], [0066]-[0068].

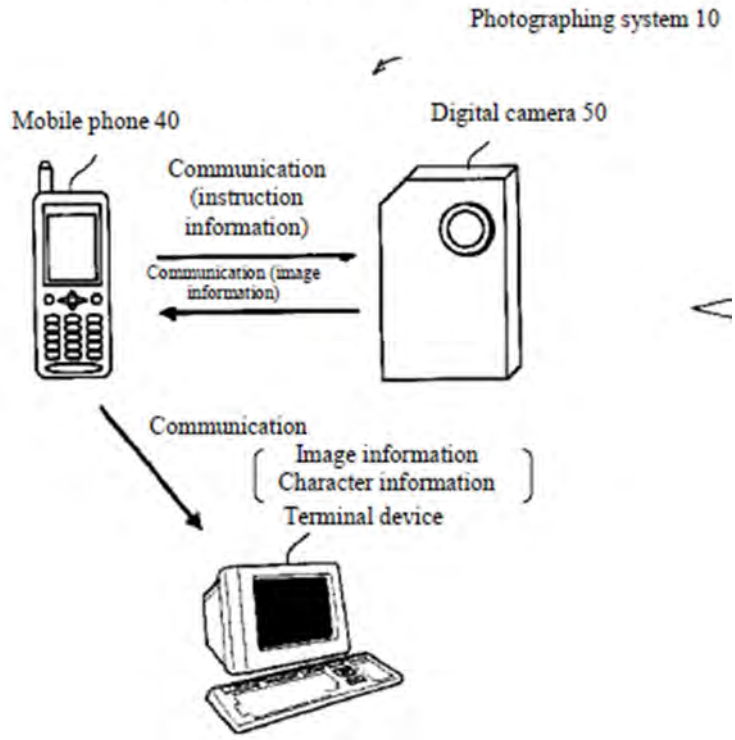
161. Hiroishi's system provides "a photographing system, a photographing method, a camera, a recording medium, and a program that allows the photographer him/herself to take a self-portrait reliably and to grasp the photographing timing correctly." Hiroishi, [0004]. Hiroishi teaches a digital camera device 50. Hiroishi, Fig. 1, Abstract ("[a] digital camera 50…."). Hiroishi further teaches a cellular phone 40 with access to the internet. *Id*., Fig. 2 (showing "mobile phone 40" connected to "Internet 12"), [0048], [0049]. Hiroishi further teaches that the digital camera is connected to the cellular phone over a wireless

connection, such as Bluetooth. *Id*., [0066] ("The photographing system 10 … is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth."), Fig 1. Hiroishi teaches a mobile phone (***Bluetooth enabled mobile phone***) that communicates with a digital camera over a Bluetooth connection. The mobile phone receives photographs from the camera and send the photographs to the remote server via a cellular network connection.



162. In FIG. 1, Hiroishi illustrates a "basic configuration of the photographing system 10." Hiroishi, [0126].

(FIG. 1)

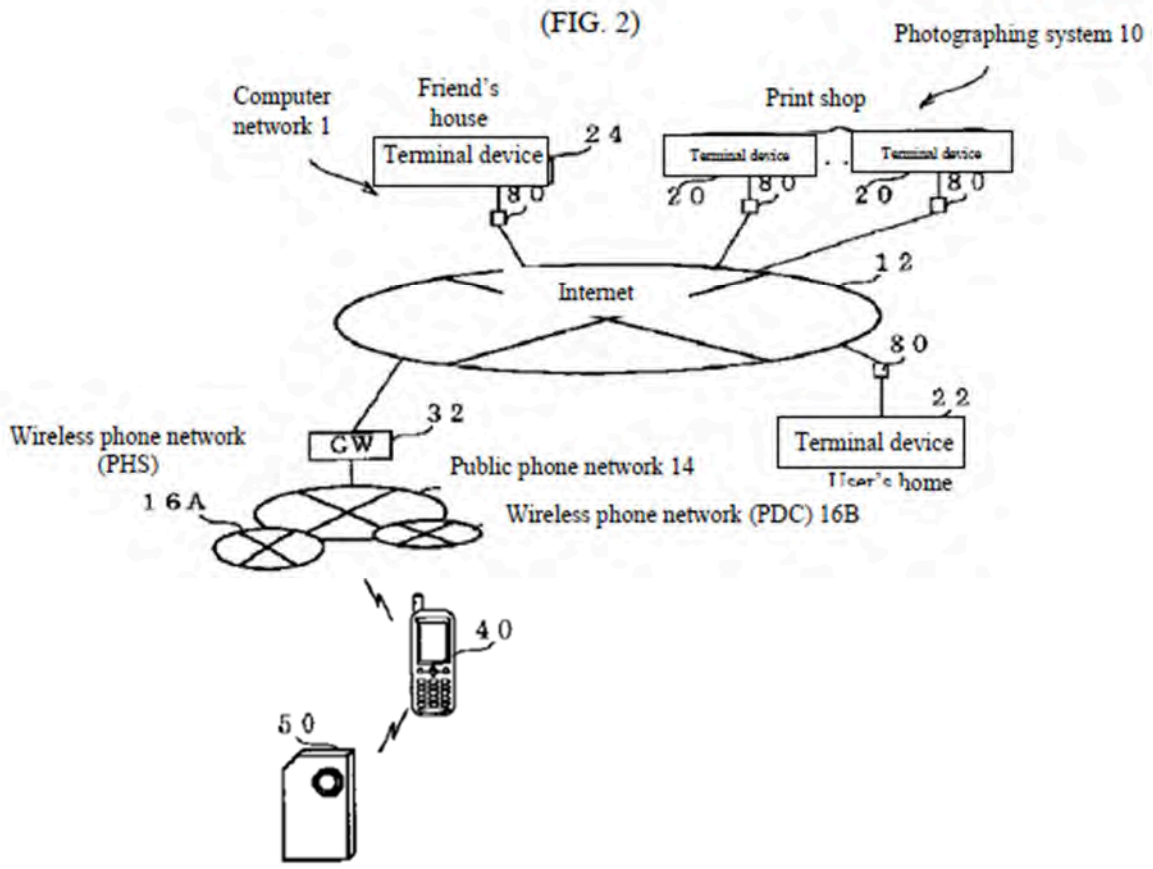


163. Hiroishi teaches that "the mobile phone 40 is configured so as to be mutually connected by a bus with a CPU (central processing unit) 41 that is responsible for the entire operation of the mobile phone 40; a ROM 42 for recording various control programs, parameters, and so forth; a RAM 43 used as a work area, or the like, at the time of execution of various control programs . . . ." Hiroishi, [0051].

164. Hiroishi teaches "[a] recording medium, capable of being read by a computer in which a program that controls the operation of a camera is installed." Hiroshi, Claim 10. Hiroishi lists the various instructions that the Bluetooth enabled cellular phone can send to the digital camera over the Bluetooth

connection to control the digital camera. Hiroishi, [0068]-[0069].

165. In FIG. 2, Hiroishi illustrates "the photographing system 10" connected to a "computer network 1" through "internet 12". Hiroishi, [0046]-[0047], FIG. 2. Hiroishi, [0048] ("Interconnection of the Internet 12 and the public telephone network 14… can provide function services, such as transmission and reception functions of data to a mobile phone 40, a caller ID authentication function , and other functions."), Abstract ("the digital camera 50 transmits to the mobile phone 40 the image information stored in the storage means, and in response to this, the mobile phone 40 transfers to a terminal device the image information received from the digital camera 50 together with the character information.").



Hiroishi, FIG. 2.

166. The terminal devices 20, 22, and 24 are computers that are part of the computer network 1, as shown in FIG. 2. Hiroishi, [0047]. The terminals 20, 22, and 24 are each connected to a network, making the terminals accessible to the cellular phone remotely. A POSITA would have understood that the terminals 20, 22, 24 to be remote servers as claimed. Note that the term "remote server" is not defined by the '030 patent specification. At best, the '030 patent describes a publishing service connected to a network. The terminal devices 20, 22, 24 are likewise connected to a network (the Internet), making them computers that are

remotely accessible to the cellular phone. As an example, the terminal device 20 includes a computer at a print shop, which is a publishing service.

167. Hiroishi's mobile phone 40 (***Bluetooth enabled mobile device***) transfers data to a terminal device (for example, ***a remote internet server***) using a cellular network. For example, Hiroishi teaches that the interconnection of the "Internet 12 and the public telephone network 14 is established by a gateway system 32." Hiroishi, [0048]. The telephone network includes a "Personal Digital Cellular" system. *Id*. The wireless telephone networks 16A and 16B can provide "transmission and reception functions of data to a mobile phone 40." *Id*.

168. According to Hiroishi, "the photographing system 10 according to this embodiment is configured to include a mobile phone 40 and a digital camera 50 configured so as to allow two-way communication, and a terminal device configured so as to allow two-way communication with the mobile phone 40." Hiroishi, [0042]. In Hiroishi's photographing system 10 "the mobile phone 40 forwards the image information received from the digital camera 50 to a terminal device." *Id*., [0044]

[12.1] providing a software module on the Bluetooth enabled mobile device, wherein the software module on the Bluetooth enabled mobile device is configured to perform steps comprising:

169. The Hiroishi-Takahashi combination renders obvious step [12.1]. *Supra* [12.P]. The Hiroishi-Takahashi combination provides a software module

(Hiroishi's "control programs" or programs that control the operation of the mobile phone as modified by Takahashi) on the Bluetooth enabled mobile device (mobile phone 40). Hiroishi, [0051], Claim 10, Takahashi, [0055], [0091], FIG. 2.

170. In my opinion, Hiroishi-Takahashi teaches providing a software module on the Bluetooth enabled mobile device. For example, Hiroishi teaches that "the mobile phone 40 is configured so as to be mutually connected by a bus with a CPU (central processing unit) 41 that is responsible for the entire operation of the mobile phone 40; a ROM 42 for recording various control programs, parameters, and so forth; a RAM 43 used as a work area, or the like, at the time of execution of various control programs . . . ." Hiroishi, [0051].

171. Hiroishi teaches "[a] recording medium, capable of being read by a computer in which a program that controls the operation of a camera is installed." Hiroshi, Claim 10. A POSITA would have understood that Hiroishi's program would be an alternative term for the software module. A POSITA would have understood that the mobile phone 40 would have implemented the software module to execute the program (or set of instructions).

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

[12.2] establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein paired secure Bluetooth connection uses cryptographic encryption key;

173. The Hiroishi-Takahashi combination renders obvious step [12.2] per the Bluetooth specification. In my opinion, the Hiroishi-Takahashi combination's software module on the Bluetooth enabled mobile device is configured to perform the step of establishing a paired secure connection (a two-way Bluetooth connection) between the Bluetooth enabled mobile device (Hiroishi's cellular phone 40) and a Bluetooth enabled data capture device (Hiroishi's digital camera 50), wherein the paired secure Bluetooth connection uses cryptographic encryption key(s).

174. For example, Hiroishi discloses "photographing system 10 …is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth… and can perform transfer of data signals." Hiroishi, [0066]-[0067]. The connection is paired because it allows two-way communication between the digital camera 50 and cellular phone 40. *Id*., [0066]. In FIG. 5, Hiroishi illustrates remote control of the digital camera by the cellular phone. Hiroishi, FIG. 5, [0071]-[0078]. In steps 100 and 104, the camera determines whether it is under remote control of the phone via the Bluetooth connection. *Id*. *See also*, Hiroishi, [0070], [0074]-[0088], [0091]-[0107], [0121].

175. To the extent the Patent Owner argues that Hiroishi does not expressly disclose that the Bluetooth pairing between the cellular phone and the digital camera includes using a cryptographic encryption key, it would have been obvious to a POSITA to modify Hiroishi to include this limitation. The use of such cryptographic encryption keys was a standard and well known part of the Bluetooth specification. For example, as discussed in the Bluetooth Core Specification V2.1, pairing between Bluetooth devices includes the generation and exchange of initialization keys created from a PIN, a random number, and a Bluetooth Device Address (BD_ADDR):

176. Referring to Bluetooth Core Specification 2.1 (July 2007), the pairing processes uses the BD_ADDR to form the initialization key (Kinit):

4.2.2 Pairing

When two devices do not have a common link key an initialization key (K_{init}) shall be created based on a PIN, and a random number and a BD_ADDR. K_{init} shall be created as specified in [Part H] Section 6.3 on page 805. When both devices have calculated K_{init} the link key shall be created, and a mutual authentication is performed. The pairing procedure starts with a device sending an LMP_in_rand PDU; this device is referred to as the "initiating LM" or "initiator" in Section 4.2.2.1 on page 251 - Section 4.2.2.5 on page 253. The other device is referred to as the "responding LM" or "responder". The PDUs used in the pairing procedure are:

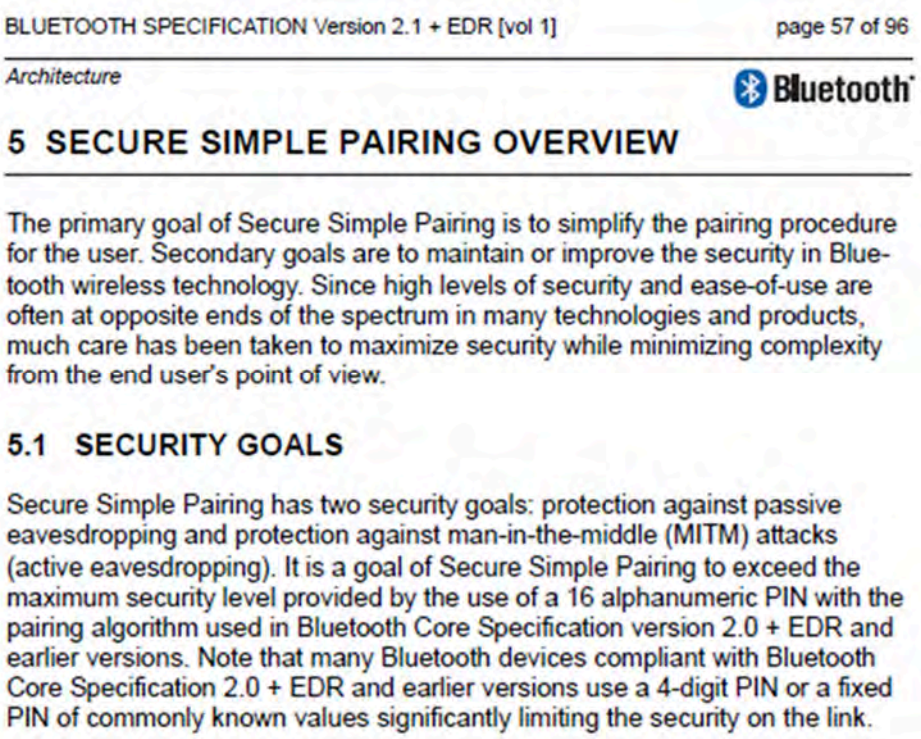
M/O	PDU	Contents
M	LMP_in_rand	random number
M	LMP_au_rand	random number
M	LMP_sres	authentication response
M	LMP_comb_key	random number
M	LMP_unit_key	key

Table 4.13: PDUs used for pairing

All sequences described in Section 4 on page 233, including the mutual authentication after the link key has been created, shall form a single transaction. The transaction ID from the first LMP_in_rand shall be used for all subsequent sequences.

E.g., Bluetooth Core Specification, 412-417 (Pairing).

177. In another example, the Bluetooth Core specification describes the process for establishing a secure pairing as well as the obvious reasons behind secure pairing such as the prevention of eavesdropping..



BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 1] page 57 of 96

Architecture

Bluetooth

5 SECURE SIMPLE PAIRING OVERVIEW

The primary goal of Secure Simple Pairing is to simplify the pairing procedure for the user. Secondary goals are to maintain or improve the security in Bluetooth wireless technology. Since high levels of security and ease-of-use are often at opposite ends of the spectrum in many technologies and products, much care has been taken to maximize security while minimizing complexity from the end user's point of view.

5.1 SECURITY GOALS

Secure Simple Pairing has two security goals: protection against passive eavesdropping and protection against man-in-the-middle (MITM) attacks (active eavesdropping). It is a goal of Secure Simple Pairing to exceed the maximum security level provided by the use of a 16 alphanumeric PIN with the pairing algorithm used in Bluetooth Core Specification version 2.0 + EDR and earlier versions. Note that many Bluetooth devices compliant with Bluetooth Core Specification 2.0 + EDR and earlier versions use a 4-digit PIN or a fixed PIN of commonly known values significantly limiting the security on the link.

See, e.g., Bluetooth Core Specification V2.1, 131-132.

178. The Bluetooth Core Specification also describes implementation of security at both the link layer and the application layer:

1 SECURITY OVERVIEW

Bluetooth wireless technology provides peer-to-peer communications over short distances. In order to provide usage protection and information confidentiality, the system provides security measures both at the application layer and the link layer. These measures are designed to be appropriate for a peer environment. This means that in each device, the authentication and encryption routines are implemented in the same way. Four different entities are used for maintaining security at the link layer: a Bluetooth device address, two secret keys, and a pseudo-random number that shall be regenerated for each new transaction. The four entities and their sizes are summarized in Table 1.1.

Entity	Size
BD_ADDR	48 bits
Private user key, authentication	128 bits
Private user key, encryption configurable length (byte-wise)	8-128 bits
RAND	128 bits

Table 1.1: Entities used in authentication and encryption procedures.

The Bluetooth device address (BD_ADDR) is the 48-bit address. The BD_ADDR can be obtained via user interactions, or, automatically, via an inquiry routine by a device.

The secret keys are derived during initialization and are never disclosed. The encryption key is derived from the authentication key during the authentication process. For the authentication algorithm, the size of the key used is always 128 bits. For the encryption algorithm, the key size may vary between 1 and 16 octets (8 - 128 bits). The size of the encryption key is configurable for two reasons. The first has to do with the many different requirements imposed on cryptographic algorithms in different countries – both with respect to export regulations and official attitudes towards privacy in general. The second reason is to facilitate a future upgrade path for the security without the need of a costly redesign of the algorithms and encryption hardware; increasing the effective key size is the simplest way to combat increased computing power at the opponent side.

See, e.g., Bluetooth Specification V2.1, 1025-1037.

179. Cryptographic authentication between wireless devices like a digital camera and cellular phone was routine at the time of the invention. Indeed, cryptographic authentication was part of the Bluetooth standard for years before the priority date of the ’030 Patent.

180. A POSITA would have understood the basic motivation for using

cryptographic authentication: to ensure that each device is communicating with its intended recipient and that information is protected from outsiders when transmitted between devices. A POSITA would have found this benefit directly applicable to the system disclosed Hiroishi, because it would have ensured the secure transmission of image files and related data between the two devices. Hiroishi teaches that the camera and phone implement a "predetermined communication protocol" and identifies Bluetooth as the preferred data transmission mechanism, so there would not have been any unexpected result if the camera and phone were configured to cryptographically authenticate each other.

[12.3] receiving a message from the Bluetooth enabled data capture device, corresponding to supported data capability of the Bluetooth enabled data capture device;

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

devices. *See* Bluetooth Core Specification V2.1, Section 4.3.4 (shown below).

4.3.4 Supported features

The supported features may be requested at anytime following a successful baseband paging procedure by sending the LMP_features_req PDU. Upon reception of an LMP_features_req PDU, the receiving device shall return an LMP_features_res PDU.

The number of features bits required will in the future exceed the size of a single page of features. An extended features mask is therefore provided to allow support for more than 64 features. Support for the extended features mask is indicated by the presence of the appropriate bit in the LMP features mask. The LMP_features_req_ext and LMP_features_res_ext PDUs operate in precisely the same way as the LMP_features_req and LMP_features_res PDUs except that they allow the various pages of the extended features mask to be requested. The LMP_features_req_ext may be sent at any time following the exchange of the LMP_features_req and LMP_features_rsp PDUs.

The LMP_features_req_ext PDU contains a feature page index that specifies which page is requested and the contents of that page for the requesting device. Pages are numbered from 0-255 with page 0 corresponding to the normal features mask. Each page consists of 64 bits. If a device does not support any page number it shall return a mask with every bit set to 0. It also contains the maximum features page number containing any non-zero bit for this device. The recipient of an LMP_features_req_ext PDU shall respond with an LMP_features_res_ext PDU containing the same page number and the appropriate features page along with its own maximum features page number.

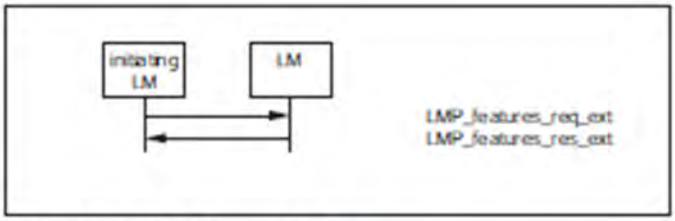
If the extended features request is not supported then all bits in all extended features pages for that device shall be assumed to be zero.

M/O	PDU	Contents
M	LMP_features_req	features
M	LMP_features_res	features
O(63)	LMP_features_req_ext	features page max supported page extended features
O(63)	LMP_features_res_ext	features page max supported page extended features

Table 4.22: PDUs used for features request.



Sequence 68: Request for supported features.



Sequence 69: Request for extended features.

E.g., Bluetooth Core Specification V2.1, 441-442.

182. As shown above, the ***max supported page*** is indicative of supported data capability of the Bluetooth enabled mobile device. Other examples of features that are reported include number of slots per packet (3 slot packets or 5 slot packets), Adaptive Frequency Hopping (AFH) capability, Channel Quality Driven Data Rate, and Enhanced Data Rate (EDR). Bluetooth Core Specification V2.1, 384-387 (explaining feature definitions).

183. A POSITA would have been motivated to use the supported data

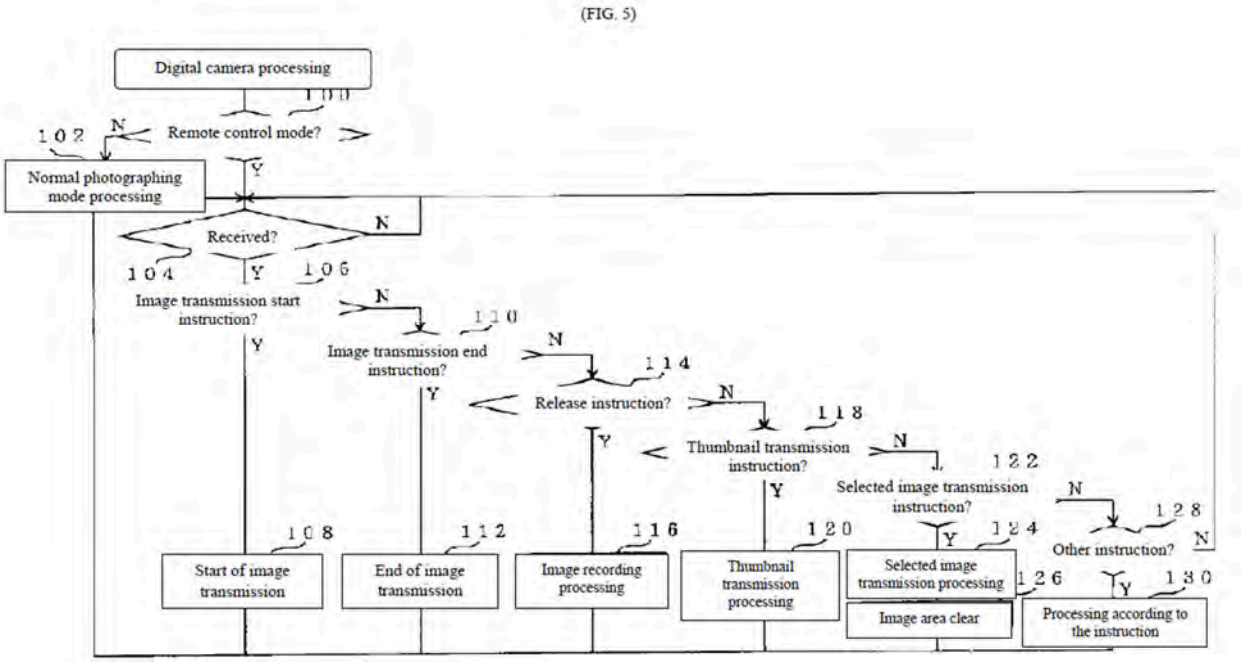
capabilities feature of the Bluetooth specification because it is essential to match the supported data capabilities of the Bluetooth-enabled devices. This alignment ensures the effective establishment of communication between a mobile phone and a digital camera, thereby facilitating superior data transmission in accordance with the Bluetooth standard.

[12.4] detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:

184. The Hiroishi-Takahashi combination renders obvious step [12.4]. The Hiroishi-Takahashi combination's software module on the Bluetooth enabled mobile device is configured to perform the step of detecting new data (photographs) acquired by the Bluetooth enabled data capture device (digital camera 50) for transfer (to mobile phone 40).

185. For example, Hiroishi teaches detection of new-data by sending a "release instruction" from the cellular phone 40 to the digital camera 50 after establishing a Bluetooth connection between the camera and the phone. Hiroishi, Abstract, [0012]. Hiroishi emphasizes that "the release instruction information is the information for instructing the timing of photographing with the camera of the present invention." Hiroishi, [0034]. The release instructions from the mobile phone would allow the camera "to photograph a picture… by transmitting the release instruction information at the timing one wishes to take a photograph with the camera of the present invention. Therefore, since the timing in which the

release instruction information is transmitted serves as the photographing timing, the photographer can grasp the photographing timing correctly." Id., [0034].



Hiroishi, FIG. 5.

186. As shown above in FIG. 5, Hiroishi illustrates remote control of the digital camera by the cellular phone. Hiroishi, FIG. 5, [0071]-[0078]. In steps 100 and 104, the camera determines whether it is under remote control of the phone via the Bluetooth. Id. At step 114, the camera receives a release instruction from the phone causing it to acquire a new image. Id., Abstract ("the mobile phone 40… transmits the release instruction information to the digital camera 50"), [0034] ("it is possible to photograph a picture with a camera also at the position away from the camera, by transmitting the release instruction information at the timing one wishes to take a photograph with the camera"), [0078] ("In Step 114, a

determination is made as to whether the instruction information received in Step 104 is the release instruction information…."). A POSITA would understand that, because the release instruction is received from the phone over the Bluetooth connection, the image is acquired after the wireless connection is established. Id.

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

[12.5] sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data,
wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;

188. The Hiroishi-Takahashi combination renders obvious step [12.5]. In the Hiroishi-Takahashi combination, the detecting step (see Element [12.4]) includes sending a message (Hiroishi's thumbnail transmission instruction) to the Bluetooth enabled data capture device (Hiroishi's digital camera 50), over the established paired secure Bluetooth connection, to enable event notifications

(Hiroishi's thumbnail images) on the Bluetooth enabled data capture device corresponding to new data (full resolution photographs), wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device (mobile phone 40).

189. This limitation is broken down into constituent steps below:

[12.5.1] sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data,

190. In the claim, the cellular phone receives an event notification signal to inform the cellular phone of the existence of new data. In the Hiroishi-Takahashi-Bluetooth combination, there are a variety of signals that would perform the event notification function. For example, Hiroishi sends thumbnails to the cellular phone. Upon receipt of the thumbnails, the cellular phone is notified that the pictures represented by the thumbnails are available. In addition, it would have been obvious to include header information, metadata, or some other information with the thumbnails or in addition to the thumbnails that informs the cellular phone of the nature of the received data—that new photos are available. A person of ordinary skill would have reason to provide an event notification or designate pre-existing data as an event notification so that the cellular phone is made aware that new data is available so that it may then take appropriate actions in response.

Because thumbnails provide a straight-forward event notification to the user, a person of ordinary skill would further use the thumbnails or associated metadata as an event notification in the software running on the cellular phone.

191. For example, Hiroishi teaches sending a message (thumbnail transmission instruction) to the Bluetooth enabled camera to enable event notifications (thumbnail images). The mobile phone sends an instruction to the camera to transmit thumbnail images of the captured images stored on the camera's memory. Supra [12.4]. Specifically, Hiroishi teaches the following instructions that are sent from the mobile phone to the camera. Hiroishi, [0068] ("Image transmission end instruction information ... is the information for instructing the stop of the transmission of the digital image data started according to the image transmission start instruction information ... 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.") Specifically, Hiroishi signifies the transition from viewfinder mode to transmission mode, allowing images to be sent as thumbnails in accordance with the transmission instructions provided. TTI-1011, [0068]. Hiroishi discloses that after the mobile phone sends a thumbnail transmission instruction to the camera, the camera processes images stored in memory (i.e., the new data) to create thumbnails, and sends the thumbnails to the

mobile phone. Hiroishi, [0081]-[0082].

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

193. Hiroishi discloses that after, "the instruction information received . . . image data that can display thumbnails is created by performing a predetermined image processing to the digital image data stored in the photographed image data storage area of SDRAM 55A (not shown), a thumbnail transmission processing for transmitting the image data to the mobile phone 40 is performed, and the process returns to Step 104 thereafter…image processing performed here is as follows: the graphical data compression/ decompression unit 62 decompresses all the compressed digital image data stored in SDRAM 55A, the image data is thinned at a predetermined thinning rate, the digital image data obtained thereby is used to create the image data with which thumbnails can be displayed, and the image data

is compressed again by the graphical data compression/ decompression unit 62. Thereby, the size of the image data that can display thumbnails to be transmitted to the mobile phone 40 can be made small, enabling high-speed transmission". Id., [0081]-[0082]. Then, the thumbnails are "transmitted according to the thumbnail transmission instruction information" to the mobile phone 40., Hiroishi, [0067], [0084].

194. Thus, the mobile phone sends the camera a thumbnail transmission instruction, which is a message to enable event notifications corresponding to the new data. The full-resolution images stored in memory are the "new data," and therefore, the thumbnails are notifications of the capture of the new data. Likewise, the thumbnails "correspond" to the new data because the thumbnails are a lower resolution representation of the full-resolution captured images stored in memory on the camera.

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

8.7 SNIFF MODE

In Sniff mode, the duty cycle of the slave's activity in the piconet may be reduced. If a slave is in active mode on an ACL logical transport, it shall listen in every ACL slot to the master traffic, unless that link is being treated as a scatternet link or is absent due to hold mode. With sniff mode, the time slots when a slave is listening are reduced, so the master shall only transmit to a slave in specified time slots. The sniff anchor points are spaced regularly with an interval of T_{sniff}.

TTI-1019, 345.

196. There is a clear process for enabling event listening using sniff mode.

4.5.3.1 Master or slave requests sniff mode

Either the master or the slave may request entry to sniff mode. The process is initiated by sending an LMP_sniff_req PDU containing a set of parameters. The receiving LM shall then decide whether to reject the attempt by sending an LMP_not_accepted PDU, to suggest different parameters by replying with an LMP_sniff_req PDU or to accept the request.

TTI-1019, 457.

[12.5.2] wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;

197. Because the new data (full resolution image) is obtained in response to instructions received by the digital camera 50 from the mobile phone 40 over the Bluetooth connection, the new data is acquired by the Bluetooth enabled data capture device (digital camera 50) after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device (digital camera 50) and the Bluetooth enabled mobile device (mobile phone 40).

198. Hiroishi teaches that the mobile phone 40 and the digital camera 50

are connected by a Bluetooth connection. Hiroishi, [0066] ("The photographing system 10 according to this embodiment is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth."), [0067] ("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. In this embodiment, the communication unit 49 is built in the mobile phone 40, and the communication unit 59 is built in the digital camera 50"), [0121] ("In this embodiment, the case where Bluetooth is applied as a standard of communication for the communication unit 49 and the communication unit 59 has been described . . . ."). Further, Hiroishi discusses all of the instructions transmitted to and images received from the camera. *See, e.g.*, Hiroishi, [0073]-[0088], *see also, e.g., id.*, [0091]-[0107], [0121].

[12.6] enabling event notification listening on Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;

199. The Hiroishi-Takahashi combination renders obvious step [12.6]. In the Hiroishi-Takahashi combination, the detecting step (*see* Element [12.4]) includes enabling event notification listening (activating the mobile phone code that "waits" to receive thumbnail images from the camera) on Bluetooth enabled mobile device, to listen ("wait") for event notifications (thumbnail images) sent

from the Bluetooth enabled data capture device (digital camera 50), over the established paired secure Bluetooth connection.

200. As discussed above (see supra [12.4]), after the mobile phone sends a thumbnail transmission instruction to the camera, the mobile phone "waits" to receive the thumbnails from the camera. A POSITA would recognize this "waiting" is the mobile phone listening for the event notifications (the thumbnails). Hiroishi, [0102] ("If yes in Step 222, that is, when the operator has specified the transmission of the image transmission end instruction information, the process goes to Step 226, wherein the image transmission end instruction information is transmitted via the communication unit 49 to the digital camera 50, and the thumbnail transmission instruction information is subsequently transmitted via the communication unit 49 to the digital camera 50 in Step 228. In response thereto, the digital camera 50 stops the image transmission processing performed in Step 112 of the digital camera processing described above, the thumbnail transmission processing is subsequently performed in Step 120, and the image data for displaying thumbnails is transmitted to the mobile phone 40."), [0104] ("In the following Step 230, [the phone] **waits** until it receives the image data that can display the thumbnail from the digital camera 50 . . . .")

201. Hiroishi, [0102]-[0104] (emphasis added). This "waiting" is the mobile phone listening for event notifications. A POSITA would understand that

the term “waiting” (in step 230) in the context of the mobile phone's action after sending a thumbnail transmission instruction to the camera implies a state where the mobile phone is actively listening for event notifications, particularly for the receipt of thumbnails from the camera. This interpretation aligns with the typical operation of communication systems, where devices often enter a state of waiting or listening for incoming data or signals. In the described scenario, the mobile phone activates and remains in a listening state until it receives the data necessary to display thumbnails from the digital camera. This waiting period serves as a mechanism for the mobile phone to remain responsive to event notifications and effectively manage the data transmission process between itself and the camera. Such listening behaviors are common across various elements in similar patents within the domain, reflecting the standard practices and expectations within the field of communication protocols and device interaction.

202. See also Bluetooth sniff mode as described in Supra [12.5.1].

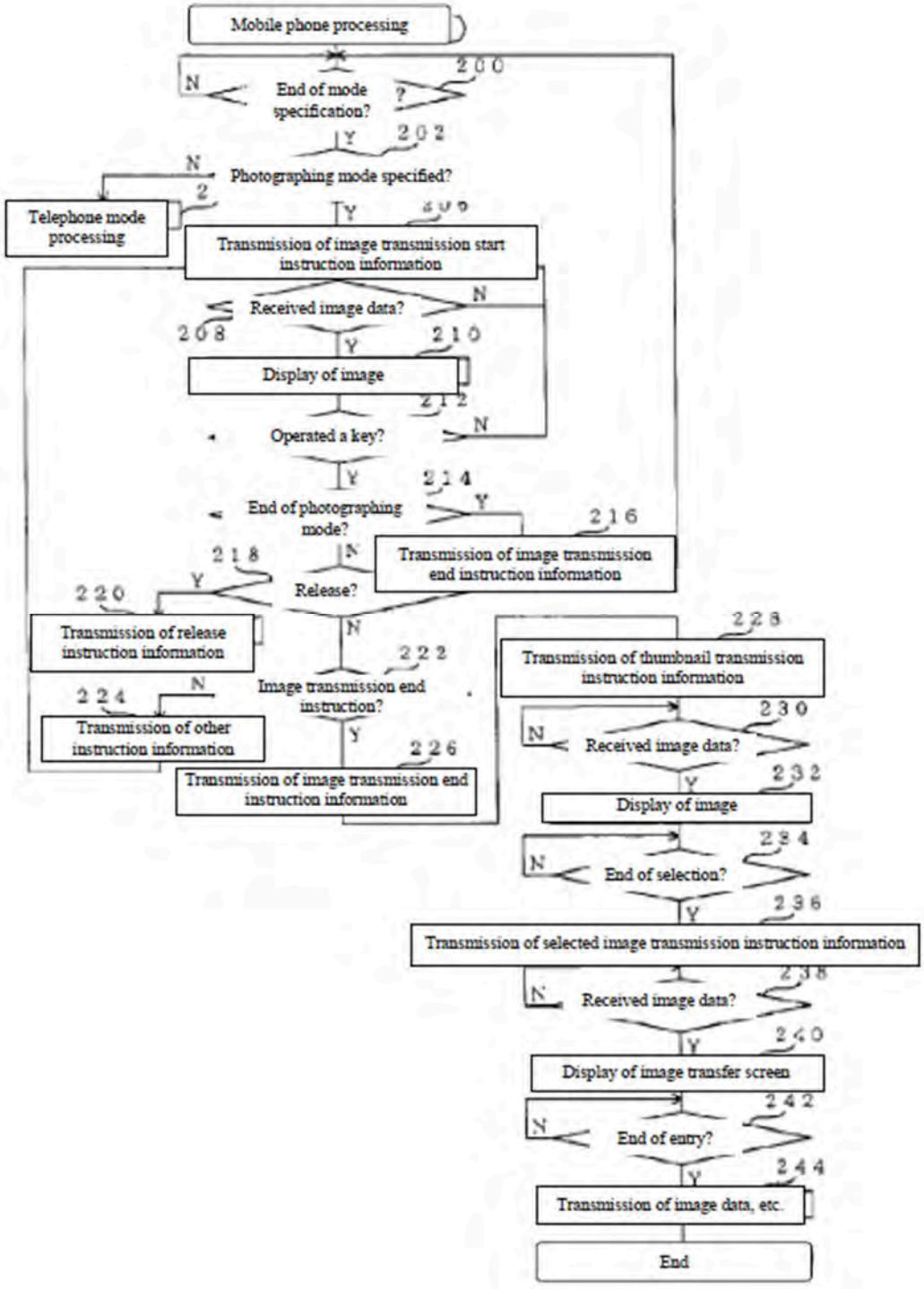
[12.7] receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and

203. The Hiroishi-Takahashi combination renders obvious element [12.7]. In the Hiroishi-Takahashi combination, the detecting step (*see* Element [12.4]) includes receiving, from the Bluetooth enabled data capture device, an event notification (thumbnail image) corresponding to existence of new data (full-

resolution image) for transfer, over the established paired secure Bluetooth connection.

204. For example, Hiroishi teaches "[a] recording medium, capable of being read by a computer in which a program that controls the operation of a camera is installed." Hiroshi, Claim 10. A POSITA would have understood that Hiroishi's program would be alternative term for the mobile software application. The program (mobile software application) is configured to wait for response (listen) for a thumbnail image (an event notification) from the camera over the Bluetooth connection as shown in Fig. 6, step 230 until the entire thumbnail is received, wherein the thumbnail (event notification) is the lower resolution image corresponding to the acquired full resolution image (new-data) and comprises sending a thumbnail over Bluetooth connection from the camera to the phone. Hiroishi, [0081]-[0082], [0104]-[0105]. A POSITA would have understood that the phone's (and/or program installed on the phone (Hiroishi, Claim 10, Abstract) "wait" action for the thumbnail images, constitutes as the phone listening for the event notification signal. See also, Supra [12.4].

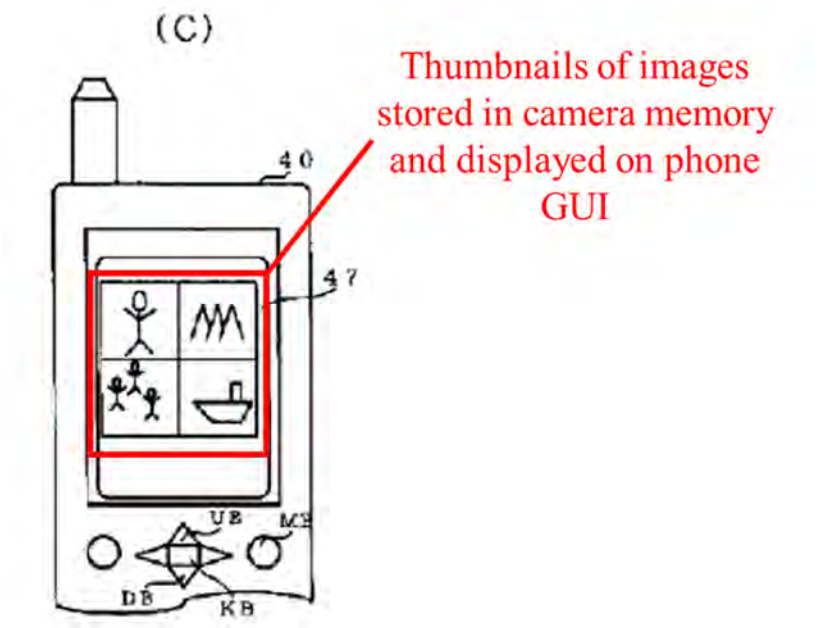
(FIG. 6)



Hiroishi, FIG. 6.

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

to the digital camera, the cellular phone "waits" for the image data in response. Hiroishi, [0102]-[0104]. Subsequently, the camera performs "thumbnail transmission… and the image data for displaying thumbnails is transmitted to the mobile phone 40." Hiroishi, [0102]. During this time, the phone "waits until it receives the image data that can display the thumbnail from the digital camera 50, and in the following Step 232, after a decompression process is performed to the received image data, the thumbnail shown according to the image data is displayed on the display unit 47 [of the phone]." Hiroishi, [0104].



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

206. The thumbnails correspond to the acquired new data (the image captured by the camera when the release instruction is given). The "image data that can display thumbnails is created by performing a predetermined image

processing to the digital image data stored in the photographed image data storage area of SDRAM 55A (not shown), a thumbnail transmission processing for transmitting the image data to the mobile phone 40 is performed, and the process returns to Step 104 thereafter." Hiroishi, [0081]-[0082]. See also, Hiroishi, claim 10, [0066]-[0068], [0121].

207. A POSITA would have also understood that the thumbnails being sent to the phone from the camera constitute the event notification. *Supra* [12.5.1].

[12.8] sending a request to the Bluetooth enabled data capture device, to get new data for transfer;

208. The Hiroishi-Takahashi combination renders obvious step [12.8]. In my opinion, Hiroishi teaches sending a request (Hiroishi's "selected image transmission instruction") to the Bluetooth enabled data capture device (digital camera 50), to get new data (full resolution images) for transfer from Hiroishi's digital camera 50 to Hiroishi's mobile phone 40.

209. For example, Hiroishi teaches the mobile phone sending a request to the camera for the new data, which are the captured images stored in the camera memory. Hiroishi teaches that the user of the mobile phone can select thumbnail images the user wants to receive from the camera. The selection of the images is an instruction sent to the camera for the camera to retrieve the images from memory, process the images, and send the images back to the mobile phone. Hiroishi, [0068] ("Selected image transmission instruction information ... is the

information for instructing the transmission of the [full resolution] digital image data corresponding to the image chosen from the [lower resolution] image shown by the thumbnails transmitted according to the thumbnail transmission instruction information by the operator of the mobile phone 40.") A POSITA would have recognized that selected image transmission instruction is the request to get new data for transfer.

[12.9] receiving, by the Bluetooth enabled mobile device, encrypted data corresponding to the new data over the established Bluetooth paired secure wireless connection and obtaining new data from the received encrypted data using cryptographic encryption key; and

210. The Hiroishi-Takahashi combination renders obvious [12.9]. In my opinion, the Hiroishi-Takahashi combination teaches receiving, by the Bluetooth enabled mobile device, encrypted data corresponding to the new data over the established Bluetooth paired secure wireless connection and obtaining new data from the received encrypted data using cryptographic encryption key (see Element [12.2]).

211. For example, Hiroishi teaches that the new data (full-resolution images stored in camera memory) are received by the mobile phone in response to the selection of thumbnails.

> Once the thumbnails are displayed on the display unit 47, an operator presses the UB, DB, or KB key provided on the mobile phone 40 to select a desired image (the image [the operator] desires to request a print shop to make prints (also see FIG. 2) or the image for which [the operator]

> desires to transmit the digital image data to a terminal unit 22 installed at home or a terminal unit 24 installed at a friend's house) from the thumbnails.
>
> Then, in the following Step 234, [the phone] waits for the end of selection of the desired image requested by the operator, and in the following Step 236, the information that can specify the image selected by the operator and the selected image transmission instruction information are transmitted to the digital camera 50 via the communication unit 49. **In response thereto, the digital camera 50 transmits to the mobile phone 40 the digital image data corresponding to the image selected** by the operator by performing the selected image transmission processing in the above described Step 124 of the digital camera processing, and then the digital image data corresponding to the image chosen by the operator in Step 126 is deleted from SDRAM 55A.
>
> In the following Step 238, [the phone] waits for the reception of the digital image data transmitted from the digital camera 50, and in the following Step 240, a predetermined image transfer screen is displayed on the display unit 47.

Hiroishi, [0105]-[0107] (emphasis added).

212. Even though the Bluetooth specification does not require data encryption, a POSITA would have found it obvious to encrypt the new data captured by the camera transmitted to the mobile phone because encryption offers numerous benefits, primarily ensuring the integrity and security of the data during transfer. Encryption also provides a safeguard against potential eavesdropping and unauthorized access, thereby preserving the confidentiality of sensitive information, such as captured images.

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

214. Moreover, it was commonplace within the field for devices to perform encryption on transmitted data to ensure secure communication channels. This established practice underscores the familiarity and feasibility of integrating encryption mechanisms into the data transmission process between the camera and the mobile phone. Once data is encrypted for transmission, decryption becomes a necessary counterpart to ensure that the recipient device can access and utilize the transmitted information. The Bluetooth specification also offers detailed insights into how to perform decryption, thereby enabling a POSITA to effectively implement the decryption process on the receiving end.

215. In summary, considering the benefits of encryption, the readily available information within the Bluetooth specification regarding encryption and decryption techniques, and the common practice of securing data transmission

through encryption, it would have been obvious to a POSITA to employ encryption for protecting the integrity and confidentiality of the data transferred from the camera to the mobile phone, as well as to implement decryption for accessing the encrypted data on the receiving device.

7 BITSTREAM PROCESSING

Bluetooth devices shall use the bitstream processing schemes as defined in the following sections.

Before the payload is sent over the air interface, several bit manipulations are performed in the transmitter to increase reliability and security. An HEC is added to the packet header, the header bits are scrambled with a whitening word, and FEC coding is applied. In the receiver, the inverse processes are carried out. Figure 7.1 on page 129 shows the processes carried out for the packet header both at the transmit and the receive side. All header bit processes are mandatory.

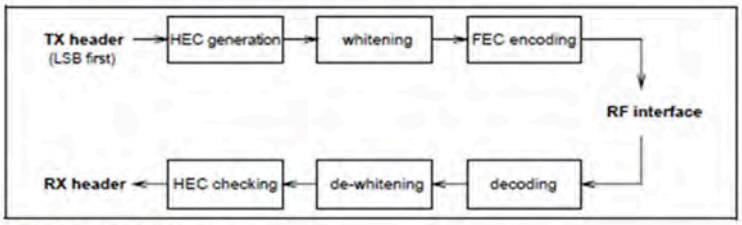


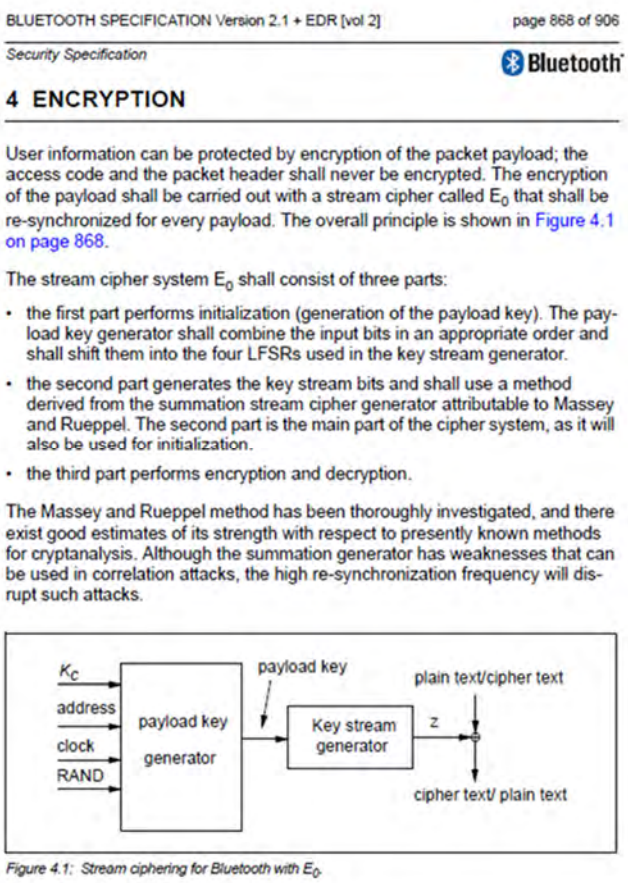
Figure 7.1: Header bit processes.

Figure 7.2 on page 129 shows the processes that may be carried out on the payload. In addition to the processes defined for the packet header, encryption can be applied on the payload. Only whitening and de-whitening, as explained in Section 7.2 on page 133, are mandatory for every payload; all other processes are optional and depend on the packet type (see Section 6.6 on page 121) and whether encryption is enabled. In Figure 7.2 on page 129, optional processes are indicated by dashed blocks.



Figure 7.2: Payload bit processes.

Bluetooth Core Specification V2.1, 299.



BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 2] page 868 of 906

Security Specification

Bluetooth

4 ENCRYPTION

User information can be protected by encryption of the packet payload; the access code and the packet header shall never be encrypted. The encryption of the payload shall be carried out with a stream cipher called E_0 that shall be re-synchronized for every payload. The overall principle is shown in Figure 4.1 on page 868.

The stream cipher system E_0 shall consist of three parts:

- the first part performs initialization (generation of the payload key). The payload key generator shall combine the input bits in an appropriate order and shall shift them into the four LFSRs used in the key stream generator.
- the second part generates the key stream bits and shall use a method derived from the summation stream cipher generator attributable to Massey and Rueppel. The second part is the main part of the cipher system, as it will also be used for initialization.
- the third part performs encryption and decryption.

The Massey and Rueppel method has been thoroughly investigated, and there exist good estimates of its strength with respect to presently known methods for cryptanalysis. Although the summation generator has weaknesses that can be used in correlation attacks, the high re-synchronization frequency will disrupt such attacks.

Figure 4.1: Stream ciphering for Bluetooth with E_0

Bluetooth Core Specification V2.1, 1038.

[12.10] transferring the obtained new data along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.

216. The Hiroishi-Takahashi combination renders obvious step [12.10].

The Hiroishi-Takahashi combination's software module on the Bluetooth enabled mobile device is configured to perform the step of transferring the obtained new

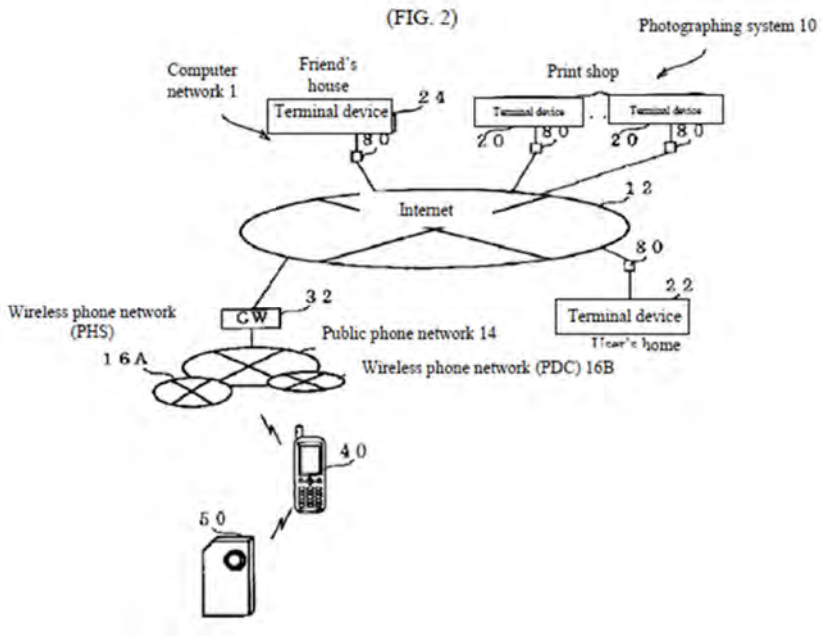
data (Hiroishi's full resolution images) along with a user identifier (email address or other identification information for the operator of the mobile phone in accordance with Takahashi) to a remote internet server (Hiroishi's terminal devices and/or an email server), wherein the transferring step comprises configuring the obtained new data (Hiroishi's full-resolution images) to comprise an action setting (Hiroishi's user instructions for a number of sheets for printing and for a scheduled pick-up date/time) and destination web address (the email address of Hiroishi's terminal device) of a remote internet server (Hiroishi's terminal devices and/or email server), wherein the action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method (HTTP in accordance with Takahashi), and wherein the user identifier uniquely identifies a particular user (the operator of Hiroishi's mobile phone 40) of the internet service provided by a remote internet server (Hiroishi's terminal devices).

217. This limitation is broken down into constituent steps below:

[12.10.1] transferring the obtained new data along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and

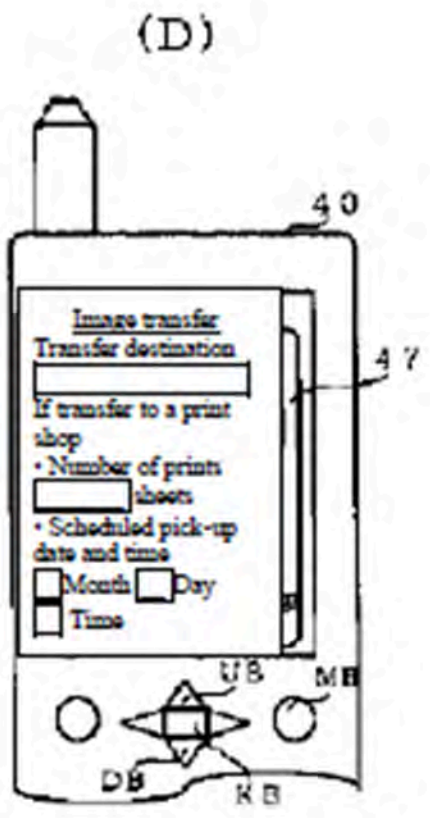
218. As discussed above, Hiroishi establishes that the mobile phone can communicate with one or more remote servers using a wireless phone network. Hiroishi teaches configuring the obtained new data with a destination web address.

In Hiroishi, the email address of the remote terminal is used for uploading the images to the remote terminal. E.g., Hiroishi, [0110].



Hiroishi, FIG. 2.

219. Hiroishi teaches configuring the obtained new data to comprise an action setting, which I understand to include commands by the user. E.g., from infringement claim chart, the "uploaded data includes the command provided by the user such as 'like' or 'scroll down.'" *E.g.*, TTI-1036, 496. The action setting of Hiroishi includes user instructions for a number of sheets for printing and a schedule pick-up date and time. E.g., Hiroishi, FIG. 7D. Hiroishi is silent as to the action setting comprising a HTTP method.



Hiroishi, FIG. 7D

220. However, a POSITA would have found it obvious to use HTTP methods for an action setting. Given the widespread use of HTTP, a POSITA would have understood that Hiroishi's mobile phone would have implemented communication with network 12 using HTTP. Specifically, it would have been obvious for Hiroishi's phone application to use HTTP (as taught by Takahashi) to transfer the received new-data (full resolution image) along with a user authentication credential (email address of the sender/phone application user) to a remote server (e.g., an email server hosting the email address of the terminal unit of the transfer destination) over a cellular data network (Hiroishi's cellular data

network).

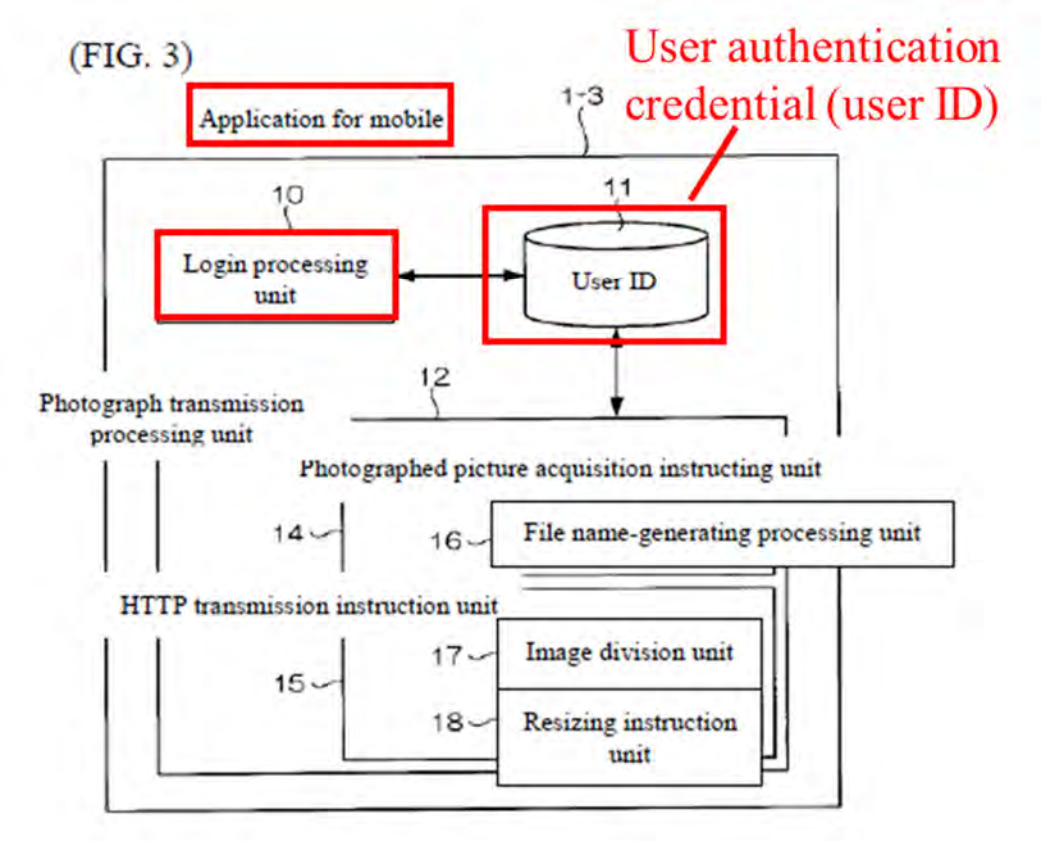
221. In my opinion, Takahashi teaches transmitting images to a remote server using HTTP. Takahashi teaches a system that allows a mobile device to use HTTP to upload image data to a remote server. Takahashi, Fig. 2, [0062] ("The image publishing processing unit 23 performs processing in publishing the image data from the mobile phone 1 to a web page."), Abstract ("a mobile telephone 1… sends the data to an image storage server 4 as an HTTP request"), [0052] ("The image storage server 4 performs a resize process of an image in order to publish the image on a web page."), [0037] ("the image data can be shared by publishing the stored image data"). The user can choose what images to publish and share. Id., [0063] ("The image selection screen generating unit 26 generates an image selection screen for allowing the user of the mobile phone 1 to select the publishable image data from among the stored image data.").

[12.10.2] wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.

222. A POSITA would have found it obvious to also include an email address or other identification information for the operator of the mobile phone with the images sent to the remote server, such as the print shop, so that images could be associated with the operator. Even though Hiroishi discusses using caller ID to authenticate the operator when collecting the printouts, a POSITA would have recognized that the photographic system would have benefited from some

identifying information associated with the images when they are transferred to the remote server. Otherwise, how would the print shop know which images belong to which operator. After the images are identified as being for the operator, the operator can then be authenticated using the caller ID.

223. For example, in the same field of endeavor, Takahashi discloses a "mobile terminal with a login processing means for logging-in to the server". Takahashi, [0010].



Takahashi, FIG. 3 (annotated).

224. After the initial configuration of the user account, Takahashi clearly discloses that login processing unit would have stored user ID locally within the

memory of the mobile phone. Id, [0055] ("The login process unit 10 stores in the user ID storage unit 11 the user ID acquired from an access to the image storage server 4 in launching the application for mobile 1-3."). This stored device identifier enables the user to access the online service provider in subsequent interactions with the remote server. Id.

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

[15.P] A method for transferring data to a remoter internet server by a Bluetooth enabled mobile device comprising:

226. To the extent the preamble is limiting, the Hiroishi-Takahashi combination renders obvious [15.P]. In my opinion, Hiroishi-Takahashi teaches a method for transferring data to a remoter internet server by a Bluetooth enabled mobile device. Supra [12.P].

[15.1] performing at a Bluetooth enabled mobile device:

227. The Hiroishi-Takahashi combination renders obvious [15.1]. In my opinion, Hiroishi-Takahashi teaches performing at a Bluetooth enabled mobile device. Supra [12.1].

[15.2] establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein the secure paired Bluetooth connection uses cryptographic encryption key;

228. The Hiroishi-Takahashi combination renders obvious [15.2]. In my opinion, Hiroishi-Takahashi teaches establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein the secure paired Bluetooth connection uses cryptographic encryption key. Supra [12.2].

[15.3] detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:

229. The Hiroishi-Takahashi combination renders obvious [15.3]. In my opinion, Hiroishi-Takahashi teaches detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer. Supra [12.4].

[15.4] sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device

230. The Hiroishi-Takahashi combination renders obvious [15.4]. In my opinion, Hiroishi-Takahashi teaches sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing

connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device. Supra [12.5].

[15.5] enabling event notification listening on the Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;

231. The Hiroishi-Takahashi combination renders obvious [15.5]. In my opinion, Hiroishi-Takahashi teaches enabling event notification listening on the Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection. Supra [12.6].

[15.6] receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and

232. The Hiroishi-Takahashi combination renders obvious [15.6]. In my opinion, Hiroishi-Takahashi teaches receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection. Supra [12.7].

[15.7] sending a request to the Bluetooth enabled data capture device, to get new data object for transfer,
wherein new data object comprises of new data, data associated with new data and time-stamp, and
wherein the time-stamp corresponds to a time when new data was acquired;

233. The Hiroishi-Takahashi combination renders obvious [15.7]. In my opinion, Hiroishi-Takahashi teaches sending a request to the Bluetooth enabled data capture device, to get new data object for transfer, wherein new data object

comprises of new data, data associated with new data and time-stamp, and wherein the time-stamp corresponds to a time when new data was acquired. Supra [12.8]. For example, Takahashi discloses that the new data picture is saved in a file along with a first time-stamp of the time the picture was taken. TTI-1014, [0070], ("The captured photograph is acquired if a photograph has been taken (Sb4). At this time, a file name is generated using the user ID stored at the time of login, and the time and date that can be acquired").

[15.8] receiving, by the Bluetooth enabled mobile device, encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection;

234. The Hiroishi-Takahashi combination renders obvious [15.8]. In my opinion, Hiroishi-Takahashi teaches receiving, by the Bluetooth enabled mobile device, encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection. Supra [12.9].

[15.9] obtaining new data, data associated with new data and time-stamp from the received encrypted data object using cryptographic encryption key; and

235. The Hiroishi-Takahashi combination renders obvious [15.9]. In my opinion, Hiroishi-Takahashi teaches obtaining new data, data associated with new data and time-stamp from the received encrypted data object using cryptographic encryption key. For example, Takahashi discloses that the new data picture is saved in a file along with a first time-stamp of the time the picture was taken. TTI-1014, [0070], ("The captured photograph is acquired…a file name is generated

using the user ID…and the time and date that can be acquired using an internal clock."). Secondly, Takahashi discloses adding another (second) time-stamp when a new data picture is selected from among a plurality of pictures to be transmitted to the image server 4. TTI-101, [0087], ("a photograph to be transmitted to the image storage server 4 is selected from a plurality of photographs… a desired photograph is chosen… a file name is generated using the user ID and the date and time"). Thirdly, Takahashi discloses that when the new data picture is published, an email (that a POSITA would understand to contain a third time-stamp) is sent (" image storage server 4 generates the URL of the web page on which the image selected on the mobile phone side is published (Sf8), and the e-mail containing the generated URL is transmitted to the selected destination"). As I described, in the Hiroishi-Takahashi system, the new data picture received by the mobile device is encrypted. Supra [12.9].

[15.10] sending the obtained new data and the obtained time-stamp along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server,
wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.

236. The Hiroishi-Takahashi combination renders obvious [15.10]. In my opinion, Hiroishi-Takahashi teaches sending the obtained new data and the obtained time-stamp along with a user identifier to a remote internet server,

comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server. Supra [12.10], [15.9].

[1.P] A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:

237. To the extent the preamble is limiting, the Hiroishi-Takahashi combination renders obvious [1.P]. In my opinion, Hiroishi-Takahashi teaches a method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device. Supra [12.P].

[1.1] performing at a Bluetooth enabled data capture device:

238. The Hiroishi-Takahashi combination renders obvious [1.1]. In my opinion, Hiroishi-Takahashi teaches performing at a Bluetooth enabled data capture device. Supra [12.1].

[1.2] establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;

239. The Hiroishi-Takahashi combination renders obvious [1.2]. In my opinion, Hiroishi-Takahashi teaches 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. Supra [12.2].

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

240. The Hiroishi-Takahashi combination renders obvious [1.3]. In my opinion, Hiroishi-Takahashi teaches sending a message to the Bluetooth enabled mobile device, corresponding to supported data capability of the Bluetooth enabled data capture device. [Supra 12.3].

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

241. The Hiroishi-Takahashi combination renders obvious [1.4]. In my opinion, Hiroishi-Takahashi teaches acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established. [Supra 12.4].

[1.5] detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device,
wherein detecting and signaling the new data for transfer comprises:

242. The Hiroishi-Takahashi combination renders obvious [1.5]. In my opinion, Hiroishi-Takahashi teaches detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer. [Supra 12.5].

[1.6] receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection;

243. The Hiroishi-Takahashi combination renders obvious [1.6]. In my opinion, Hiroishi-Takahashi teaches receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection. [Supra 12.8].

[1.7] receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection;

244. The Hiroishi-Takahashi combination renders obvious [1.7]. In my opinion, Hiroishi-Takahashi teaches receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection. [Supra 12.5].

[1.8] enabling event notification on Bluetooth enabled data capture device, corresponding to new data;

245. The Hiroishi-Takahashi combination renders obvious [1.8]. In my opinion, Hiroishi-Takahashi teaches enabling event notification on Bluetooth enabled data capture device, corresponding to new data. [Supra 12.5].

[1.9] determining existence of the new data for transfer; and

246. The Hiroishi-Takahashi combination renders obvious [1.9]. In my opinion, Hiroishi-Takahashi teaches determining existence of the new data for

transfer. [Supra 12.7].

[1.10] sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection,
wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth enabled data capture device;

247. The Hiroishi-Takahashi combination renders obvious [1.10]. In my opinion, Hiroishi-Takahashi teaches sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth enabled data capture device. Supra [12.7]

[1.11] encrypting, using cryptographic encryption key, the new data acquired in the Bluetooth enabled data capture device; and

248. The Hiroishi-Takahashi combination renders obvious [1.11]. In my opinion, Hiroishi-Takahashi teaches encrypting, using cryptographic encryption key, the new data acquired in the Bluetooth enabled data capture device. [Supra 12.9].

[1.12] transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection,
wherein the Bluetooth enabled mobile device has access to the internet,
wherein the Bluetooth enabled mobile device is configured to receive the encrypted data and obtain the new data from the encrypted data using cryptographic encryption key,
wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the

obtained new data,
wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method,
wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server,
wherein the user identifier uniquely identifies a particular user of internet service provided by the remote internet server.

249. The Hiroishi-Takahashi combination renders obvious [1.12]. In my opinion, Hiroishi-Takahashi teaches transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data and obtain the new data from the encrypted data using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by the remote internet server.. Supra [12.10].

[6.P] A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:

250. To the extent the preamble is limiting, the Hiroishi-Takahashi combination renders obvious [6.P]. In my opinion, Hiroishi-Takahashi teaches a method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device. Supra [1.P].

[6.1] performing at a Bluetooth enabled data capture device:

251. The Hiroishi-Takahashi combination renders obvious [6.1]. In my opinion, Hiroishi-Takahashi teaches performing at a Bluetooth enabled data capture device. Supra [1.1].

[6.2] establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;

252. The Hiroishi-Takahashi combination renders obvious [6.2]. In my opinion, Hiroishi-Takahashi teaches 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. Supra [1.2].

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

253. The Hiroishi-Takahashi combination renders obvious [6.3]. In my opinion, Hiroishi-Takahashi teaches acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure

Bluetooth connection is established. Supra [1.4].

[6.4] detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device,
wherein detecting and signaling the new data for transfer comprises:

254. The Hiroishi-Takahashi combination renders obvious [6.4]. In my opinion, Hiroishi-Takahashi teaches detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer. Supra [1.5].

[6.5] receiving a message from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, to register for data signal notifications,
wherein the data signal notifications correspond to existence of new data for transfer on the Bluetooth enabled data capture device;

255. The Hiroishi-Takahashi combination renders obvious [6.5]. In my opinion, Hiroishi-Takahashi teaches receiving a message from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, to register for data signal notifications, wherein the data signal notifications correspond to existence of new data for transfer on the Bluetooth enabled data capture device. Supra [12.6]. As discussed above (see supra [12.4]), after the mobile phone sends a thumbnail transmission instruction to the camera, the mobile phone "waits" to receive the thumbnails from the camera. A POSITA would recognize this thumbnail transmission instruction to the camera as the mobile phone registering for the data signal notifications (the thumbnails).

[6.6] determining existence of the new data for transfer; and

256. The Hiroishi-Takahashi combination renders obvious [6.6]. In my opinion, Hiroishi-Takahashi teaches determining existence of the new data for transfer. Supra [1.9].

[6.7] creating a new data object on the Bluetooth enabled data capture device, wherein the new data object comprises new data, data associated with new data and a data signal notification,
wherein data signal notification is a time-stamp attribute inside the data object,
wherein the data signal notification corresponds to existence of new data for transfer, and
wherein the time-stamp corresponds to a time when new data was acquired;

257. The Hiroishi-Takahashi combination renders obvious [6.7]. In my opinion, Hiroishi-Takahashi teaches creating a new data object on the Bluetooth enabled data capture device, wherein the new data object comprises new data, data associated with new data and a data signal notification, wherein data signal notification is a time-stamp attribute inside the data object, wherein the data signal notification corresponds to existence of new data for transfer, and wherein the time-stamp corresponds to a time when new data was acquired. For example, Takahashi discloses that the new data picture is saved in a file along with a first time-stamp of the time the picture was taken. TTI-101, [0070], ("The captured photograph is acquired…a file name is generated using the user ID…and the time and date"). *See also* Supra [15.9].

[6.8] encrypting, using cryptographic encryption key, the new data object in the Bluetooth enabled data capture device; and

258. The Hiroishi-Takahashi combination renders obvious [6.8]. In my opinion, Hiroishi-Takahashi teaches encrypting, using cryptographic encryption key, the new data object in the Bluetooth enabled data capture device. Supra [1.11].

[6.9] transferring the encrypted data object from the Bluetooth enabled data capture device to the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection,
wherein the Bluetooth enabled mobile device has access to the internet,
wherein the Bluetooth enabled mobile device is configured to receive the encrypted data object and obtain the new data and the data signal notification from the encrypted data object using cryptographic encryption key,
wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data,
wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method,
wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server,
wherein the user identifier uniquely identifies a particular user of internet service provided by a remote internet server.

259. The Hiroishi-Takahashi combination renders obvious [6.9]. In my opinion, Hiroishi-Takahashi teaches transferring the encrypted data object from the Bluetooth enabled data capture device to the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data object and obtain the new

data and the data signal notification from the encrypted data object using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by a remote internet server. Supra [1.12].

260. The ***"data signal notification***" is disclosed by Hiroishi as the thumbnails that are "transmitted according to the thumbnail transmission instruction information" to the mobile phone 40., Hiroishi, [0067], [0084]. The mobile phone sends the camera a thumbnail transmission instruction, which is a message to enable the "data signal notification" corresponding to the new data. The full-resolution images stored in memory are the "new data," and therefore, the thumbnails are the "data signal notification" of the capture of the new data. Likewise, the thumbnails "correspond" to the new data and serve as a data signal notification because the thumbnails are a lower resolution representation of the full-resolution images stored in memory on the camera.

[2] The method of claim 1, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.

261. The Hiroishi-Takahashi combination renders obvious [2]. In my opinion, Hiroishi-Takahashi teaches Bluetooth capability is provided internally in the Bluetooth enabled data capture device. For example, Hiroishi teaches that the camera includes an internal short-range wireless communications module, TTI-1011, Fig. 4, [0058], ("The digital camera 50 is further provided with…a communication unit 59 for performing communication corresponding to the predetermined communication protocol with the mobile phone 40."), TTI-1011, [0067], ("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.").

[7] The method of claim 6, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.

262. The Hiroishi-Takahashi combination renders obvious [7]. In my opinion, Hiroishi-Takahashi teaches Bluetooth capability is provided internally in the Bluetooth enabled data capture device. Supra [2].

[11] The method of claim 6, wherein the time-stamp is either absolute time or relative time.

263. The Hiroishi-Takahashi combination renders obvious [11]. In my opinion, Hiroishi-Takahashi teaches the time-stamp is either absolute time or relative time. For example, Takahashi discloses that the new data picture is saved in a file along with a first time-stamp of the time the picture was taken. TTI-101,

[0070], ("The captured photograph is acquired…a file name is generated using the user ID…and the time and date"). See also Supra [15.9]. A POSITA would understand that Takahashi's time and date is a time-stamp in absolute time.

[13] The method of claim 12, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

264. The Hiroishi-Takahashi combination renders obvious [13]. In my opinion, Hiroishi-Takahashi teaches the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data. For example, Hiroishi discloses the new data can be at least image data, TTI-1011, [0068], [0079], [0093] and video data but states that the embodiment is not limited to still pictures. Id., [0123].

[4] The method of claim 1, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

265. The Hiroishi-Takahashi combination renders obvious [4]. In my opinion, Hiroishi-Takahashi teaches the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data. Supra [13].

[9] The method of claim 6, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

266. The Hiroishi-Takahashi combination renders obvious [9]. In my opinion, Hiroishi-Takahashi teaches the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data. Supra [13].

[14] The method of claim 12, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

267. The Hiroishi-Takahashi combination renders obvious [14]. In my opinion, Hiroishi-Takahashi teaches event notification corresponds to creation of new data for transfer or change in status of new data for transfer. For example, Hiroishi discloses that after a user selects a picture transfer from the event notification thumbnail images, the full resolution image is processed by the camera for transfer to the mobile phone, TTI-1011, [0084], ("Step 124, wherein a selected image transmission processing is performed, the selected image transmission processing is that the digital image data corresponding to the image selected by the operator of the mobile phone 40 from a plurality of images shown by the thumbnails").

[5] The method of claim 1, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

268. The Hiroishi-Takahashi combination renders obvious [5]. In my opinion, Hiroishi-Takahashi teaches event notification corresponds to creation of new data for transfer or change in status of new data for transfer. Supra [14].

[10] The method of claim 6, wherein said data signal notification corresponds to creation of new data for transfer or change in status of new data for transfer.

269. The Hiroishi-Takahashi combination renders obvious [10]. In my opinion, Hiroishi-Takahashi teaches said data signal notification corresponds to creation of new data for transfer or change in status of new data for transfer. Supra [14].

[16] The method of claim 15, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

270. The Hiroishi-Takahashi combination renders obvious [16]. In my opinion, Hiroishi-Takahashi teaches the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data. Supra [13].

[17] The method of claim 15, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

271. The Hiroishi-Takahashi combination renders obvious [17]. In my opinion, Hiroishi-Takahashi teaches event notification corresponds to creation of new data for transfer or change in status of new data for transfer. Supra [14].

[18] The method of claim 6, wherein the time-stamp is either absolute time or relative time.

272. The Hiroishi-Takahashi combination renders obvious [18]. In my opinion, Hiroishi-Takahashi teaches the time-stamp is either absolute time or relative time. Supra [11]. Takahashi teaches that the time is added based on an internal clock, which could indicate relative time or absolute time. TTI-1014, [0070].

B. Ground 1B—Hiroishi in Combination with Kahn and Bluetooth 2.1 Renders Claims 1-18 Invalid

273. Hiroishi teaches a photograph system that includes a cellular phone that connects to a camera via a Bluetooth connection. The cellular phone can control the camera to capture images, store images, and transmit images to the cellular phone. The cellular phone can then transmit images to a remote computer

destination by a cellular network connection via the Internet. In the combination, the mobile phone of Hiroishi is configured to apply an action setting that includes an HTTP method to the received images from the camera, in a manner similar to what was suggested by Kahn. Also in the combination, Hiroishi sends a user identifier with the transmission of the images as taught by Kahn. In the combination, Hiroishi sends a time-stamp of when the image or images were taken, in a manner similar to what was suggested by Kahn.

274. In addition, in the combination, the Bluetooth-enabled camera of Hiroishi encrypts the image data transmitted to Bluetooth-enabled cellular phone over the Bluetooth connection using an encryption technique consistent with the teachings of the Bluetooth 2.1 Core Specification. In the combination, the camera of Hiroishi provides a message corresponding to supported device capabilities to the mobile phone (e.g., after a Bluetooth connection has been established), as described by the Bluetooth Core Specification V2.1.

3. The Predictable Combination of Hiroishi, Kahn, and Bluetooth 2.1

275. A POSITA at the time of the invention would have been motivated to combine the teachings of Hiroishi and Kahn, thus rendering the subject matter of the ’030 patent challenged claims (claims 1-2, 4-7, 9-18) obvious.

276. First, both Hiroishi and Kahn are analogous art to the claimed invention. Both references are from the same field of endeavor as the claimed

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

277. Hiroishi and Kahn are also pertinent to the problem of the '030 patent: transmission of image data by a cellular phone that was captured by a digital camera. TTI-1001, Background. Hiroishi addresses this problem through Bluetooth wireless data transmission and software-based control of the digital camera from the mobile device. *See, e.g.*, Hiroishi, [0043], [0053], [0061]. Kahn addresses the problem through efficient publishing of image data from a cellular phone to a website using HTTP. *See, e.g.*, Kahn, [0056], [0063].

278. Second, a POSITA would have been motivated to use Kahn's upload technique to publish image data received at the mobile device of Hiroishi. At the time of the alleged Critical Date, photo-sharing websites and personal blogs had become ubiquitous. *See, e.g.*, TTI-1020, 3:25-49, 4:47-67; TTI-1021, 5:49-56 (describing use HTTP to send images from the phone to the server). Websites like FLICKR, PHOTOBUCKET, and PICASA allowed users to publish photographs

and share them with friends, colleagues, and internet users. *See, e.g.*, TTI-2018, 5:25-28; TTI-2022, [0032].

279. Cellular phones had also become ubiquitous. The original iPhone was released six months before the provisional filing date of the '030 patent (the iPhone was released on June 29, 2007), and years before that companies like Blackberry, Motorola, and Nokia had developed cellular phones that allowed users to transfer image data over the Internet. *See e.g.*, Hiroishi, [0015], [0047], FIG. 2. The '030 patent even refers to mobile phones as "ubiquitous." '030 patent, 9:46-47 ("The mobile device 202 may, for example, be a **ubiquitous mobile phone**.") (emphasis added). Kahn also teaches a camera wirelessly connected to a mobile phone for capturing images and uploading images to a remote server. *See, e.g.*, Kahn, [0045], [0055].

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

281. The teachings of Kahn would have provided straightforward benefit to the user of the mobile device in Hiroishi: predictable upload of image files and an action setting using an existing HTTP connection between the mobile device and a remote (publishing) server. Hiroishi already teaches the desire to transfer image data from a digital camera to a mobile device to a terminal device. *See, e.g.*,

Hiroishi, [0044]. Kahn would have furthered this purpose by allowing the user to share image data over the Internet in a straight-forward and well-known way.

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

283. Fourth, a POSITA would have been motivated, and found it obvious, to include user identifier that uniquely identifies a particular user of the Internet service. Hiroishi already teaches that the email address of the destination terminal

is used to send images to the destination terminal. Hiroishi, [0110]. Because the 030 claims do not require that the user identifier uniquely identifies the operator of the mobile phone, Hiroishi alone would invalidate this feature. To the extent that the user identifier is interpreted to be the identifier of the user of the mobile phone, a POSITA would have found it obvious to include the user identifier with the images when transferring the images to the remote internet server. *See, e.g.*, Kahn, [0098]. This way, a POSITA would recognize the advantage of being able to uniquely identify the owner of the images, e.g., using a database field for user ID. Kahn, [0098]. In the example scenario of Hiroishi's print shop, the print shop worker can quickly and easily identify the owner of the images by the file name, and can validate the owner when providing the printed images. Likewise, the fulfillment center worker of Kahn can easily identify the owner of the images.

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

285. A POSITA would have found it obvious to modify Hiroishi to include

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

286. I note that the '030 patent specification does not provide written description support for the camera (or other data capture device) sending a time-stamp to the mobile phone. At best, the '030 patent describes the "segmentation module 203i [at the mobile phone] generates segment identifiers and tags the data

segments with the segment identifiers. The segment identifiers may, for example, be one or more of transaction identifiers, sequence numbers, and timestamps." '030 patent, 7:55-59. While I believe that the transmission of a time-stamp from the camera to the phone with the images would have been an obvious modification to Hiroishi, the '030 patent does not provide any written description support for doing so.

287. A POSITA would have also found it obvious that the camera of Hiroishi would have provided a message corresponding to supported data capability of the camera to the mobile phone upon establishment of the Bluetooth connection, in a manner consistent with the protocols described in the Bluetooth Core Specification. *See, e.g.*, Bluetooth Core Specification V2.1, 441 (4.3.4 Supported Features), 384 (3.2 Feature Definitions). A POSITA would have recognized the benefits of indicating the camera's supported data capability. For example, the mobile phone, as the "master" of the Bluetooth connection, would have used the supported data capability of the camera to configure the Bluetooth communication channel, so that communications between the camera and the mobile phone across the Bluetooth channel would be efficient and resource friendly.

288. In addition, the reporting by the camera of supported data capability includes whether the camera supports encryption. *See, e.g.*, Bluetooth Core

Specification V2.1, 386. A POSITA would have recognized the benefits of reporting whether the camera supports enhanced data rates so the devices could choose the fastest possible data rate for transferring pictures to optimize the user experience.

289. An example of supported features include, but are not limited to:

Feature	Definition
3 slot packets	This feature indicates whether the device supports the transmission and reception of both DM3 and DH3 packets for the transport of traffic on the ACL-U logical link.
5 slot packets	This feature indicates whether the device supports the transmission and reception of both DM5 and DH5 packets for the transport of traffic on the ACL-U logical link.
AFH capable slave	This feature indicates whether the device is able to support the Adaptive Frequency Hopping mechanism as a slave as defined in Baseband Specification, Section 2.3, on page 70 using the LMP sequences defined in Section 4.1.4 on page 227.
Encryption	This feature shall be supported. This feature indicates whether the device supports the encryption of packet contents using the sequence defined in Section 4.2.5 on page 248.
Enhanced Data Rate ACL 2 Mbps mode	This feature indicates whether the device supports the transmission and reception of 2-DH1 packets for the transport of traffic on the ACL-U logical link.
Enhanced Data Rate ACL 3 Mbps mode	This feature indicates whether the device supports the transmission and reception of 3-DH1 packets for the transport of traffic on the ACL-U logical link.

	This feature bit shall only be set if the "Enhanced Data Rate ACL 2 Mbps mode" feature bit is set.
3-slot Enhanced Data Rate ACL packets	This feature indicates whether the device supports the transmission and reception of three-slot Enhanced Data Rate packets on the ACLU logical link. This feature bit shall only be set if the "Enhanced Data Rate ACL 2 Mbps mode" feature bit is set.
5-slot Enhanced Data Rate ACL packets	This feature indicates whether the device supports the transmission and reception of 5-slot Enhanced Data Rate packets for the transport of traffic on the ACL-U logical link. This feature bit shall only be set if the "Enhanced Data Rate ACL 2 Mbps mode" feature bit is set.

290. Example Features Definition, Bluetooth Core Specification V2.1, 384-389.

291. I note that the limitation for transmitting a message corresponding to the supported data capability is not supported by the '030 patent specification. To the extent that the patent owner argues that transmitting a message from the camera to the mobile phone corresponding to the supported data capability is mandatory by the Bluetooth Core Specification, the claim limitation is invalid based on the combination of Hiroishi, which teaches the use of a Bluetooth connection for transmitting images from the camera to the mobile phone. *See, e.g.*, Hiroishi, [0066]-[0067].

292. A POSITA would have also found it obvious to encrypt the image data transferred from the Bluetooth-enabled camera to the cellular phone of

Hiroishi. The Bluetooth Core Specification 2.1 describes the encryption of payload data. Specifically, the Bluetooth Core Specification 2.1 states that "user information can be protected by encryption of the packet payload." TTI-1019, 1038. For example, the "encryption of the payload shall be carried out with a stream cipher called E_0 that shall be re-synchronized for every payload." *Id*.

293. A POSITA would have recognized the benefits of implementing encryption of data in the Hiroishi-Kahn combination. For example, a POSITA would have recognized that encrypting the data protected the data from being intercepted and decrypted by a malicious attacker or other unauthorized accesses. A POSITA implementing Bluetooth encryption would have had a reasonable expectation of success encrypting data. The Bluetooth Core Specification 2.1 also teaches how to activate encryption between two Bluetooth devices (*see, e.g.*, *id*., 884 ("Set Connection Encryption")), as well as how to perform encryption to protect the payload (*see, e.g.*, *id*., 919 ("1 ENCRYPTION SAMPLE DATA")). For example, the Bluetooth Core Specification 2.1 suggests a "Massey and Reuppel method." TTI-1019, 1038, 1040-1047 (providing examples of how encryption can be implemented).

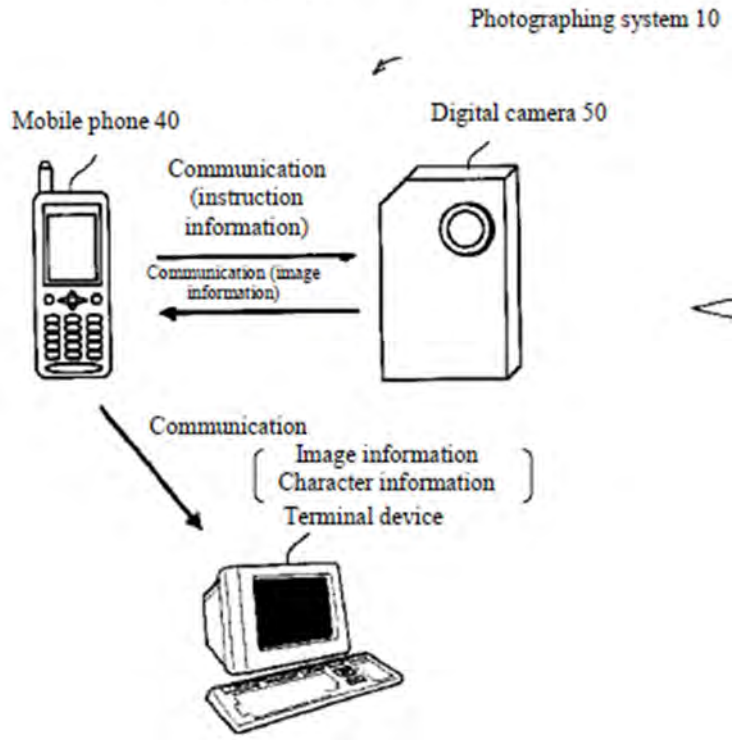
4. Analysis

Claim 12

[12.P] A method for transferring data to a remote internet server by a Bluetooth enabled mobile device comprising:

294. To the extent the preamble is limiting, the Hiroishi-Kahn-Bluetooth combination renders obvious [12.P]. Hiroishi's system provides "a photographing system, a photographing method, a camera, a recording medium, and a program that allows the photographer him/herself to take a self-portrait reliably and to grasp the photographing timing correctly." Hiroishi, [0004]. Hiroishi teaches a digital camera device 50. Hiroishi, Fig. 1, Abstract ("[a] digital camera 50…."). Hiroishi further teaches a cellular phone 40 with access to the internet. Id. Fig. 2 (showing "mobile phone 40" connected to "Internet 12"), [0048], [0049]. Hiroishi further teaches that the digital camera is connected to the cellular phone over a wireless connection, such as Bluetooth. *Id*. [0066] ("The photographing system 10… is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth."), Fig 1. Hiroishi teaches a mobile phone (***Bluetooth enabled mobile phone***) that communicates with a digital camera over a Bluetooth connection. The mobile phone receives photographs from the camera and send the photographs to the remote server via a cellular network connection. In FIG. 1, Hiroishi illustrates a "basic configuration of the photographing system 10." Hiroishi, [0126].

(FIG. 1)

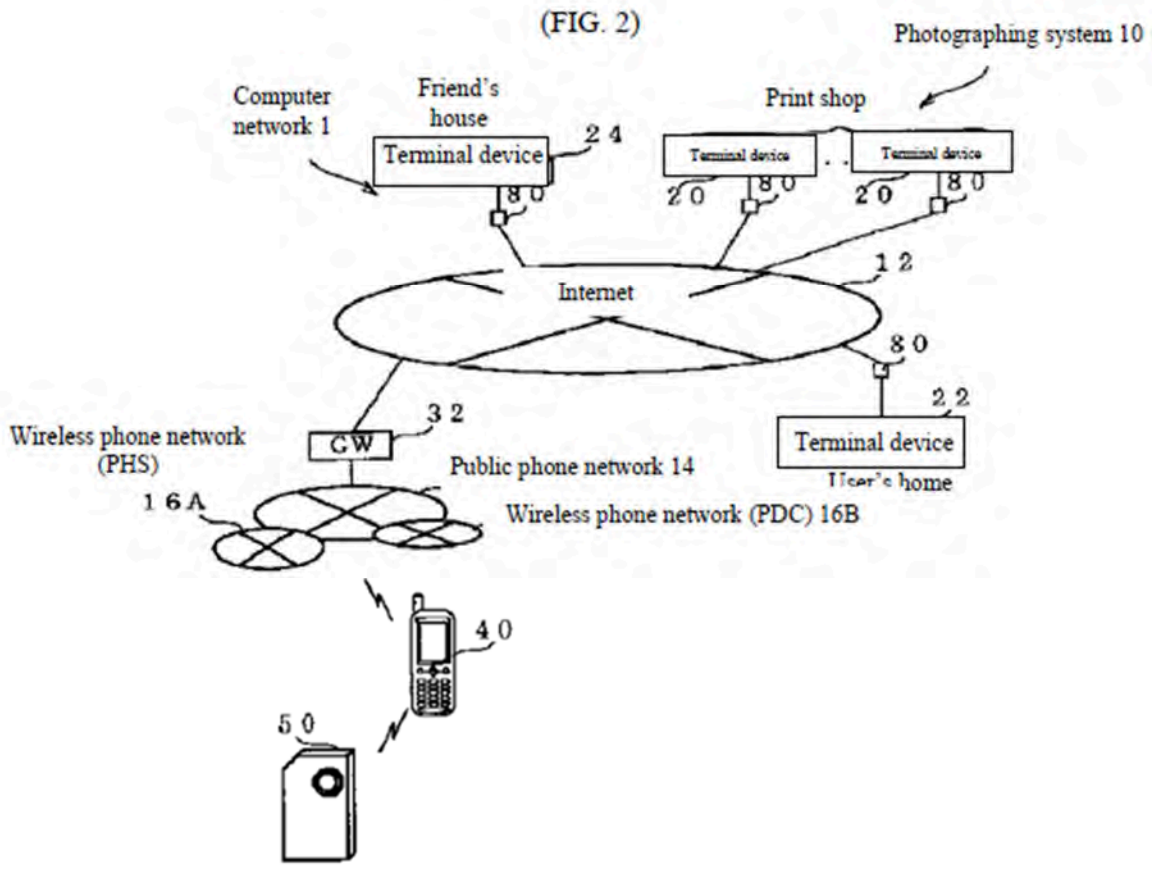


295. Hiroishi teaches that "the mobile phone 40 is configured so as to be mutually connected by a bus with a CPU (central processing unit) 41 that is responsible for the entire operation of the mobile phone 40; a ROM 42 for recording various control programs, parameters, and so forth; a RAM 43 used as a work area, or the like, at the time of execution of various control programs . . . ." Hiroishi, [0051].

296. Hiroishi teaches "[a] recording medium, capable of being read by a computer in which a program that controls the operation of a camera is installed." Hiroshi, Claim 10. Hiroishi lists the various instructions that the Bluetooth enabled cellular phone can send to the digital camera over the Bluetooth

connection to control the digital camera. Hiroishi, [0068]-[0069].

297. In FIG. 2, Hiroishi illustrates "the photographing system 10" connected to a "computer network 1" through "internet 12". Hiroishi, [0046]-[0047], FIG. 2. Hiroishi, [0048] ("Interconnection of the Internet 12 and the public telephone network 14… can provide function services, such as transmission and reception functions of data to a mobile phone 40, a caller ID authentication function , and other functions."), Abstract ("the digital camera 50 transmits to the mobile phone 40 the image information stored in the storage means, and in response to this, the mobile phone 40 transfers to a terminal device the image information received from the digital camera 50 together with the character information.")



Hiroishi, FIG. 2.

298. The terminal devices 20, 22, and 24 are computers that are part of the computer network 1, as shown in FIG. 2. Hiroishi, [0047]. The terminals 20, 22, and 24 are each connected to a network, making the terminals accessible to the cellular phone remotely. A POSITA would have understood that the terminals 20, 22, 24 to be remote servers as claimed. Note that the term "remote server" is not defined by the '030 patent specification. At best, the '030 patent describes a publishing service connected to a network. The terminal devices 20, 22, 24 are likewise connected to a network (the Internet), making them computers that are

remotely accessible to the cellular phone. As an example, the terminal device 20 includes a computer at a print shop, which is a publishing service.

299. Hiroishi's mobile phone 40 (***Bluetooth enabled mobile device***) transfers data to a terminal device (for example, ***a remote internet server***) using a cellular network. For example, Hiroishi teaches that the interconnection of the "Internet 12 and the public telephone network 14 is established by a gateway system 32." Hiroishi, [0048]. The telephone network includes a "Personal Digital Cellular" system. *Id*. The wireless telephone networks 16A and 16B can provide "transmission and reception functions of data to a mobile phone 40." *Id*.

300. According to Hiroishi, "the photographing system 10 according to this embodiment is configured to include a mobile phone 40 and a digital camera 50 configured so as to allow two-way communication, and a terminal device configured so as to allow two-way communication with the mobile phone 40." Hiroishi, [0042]. In Hiroishi's photographing system 10 "the mobile phone 40 forwards the image information received from the digital camera 50 to a terminal device." *Id*., [0044].

[12.1] providing a software module on the Bluetooth enabled mobile device, wherein the software module on the Bluetooth enabled mobile device is configured to perform steps comprising:

301. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.1]. Supra [12. P]. In my opinion, Hiroishi-Kahn-Bluetooth teaches providing a

software module on the Bluetooth enabled mobile device. For example, Hiroishi teaches that "the mobile phone 40 is configured so as to be mutually connected by a bus with a CPU (central processing unit) 41 that is responsible for the entire operation of the mobile phone 40; a ROM 42 for recording various control programs, parameters, and so forth; a RAM 43 used as a work area, or the like, at the time of execution of various control programs . . . ." Hiroishi, [0051].

302. Hiroishi teaches "[a] recording medium, capable of being read by a computer in which a program that controls the operation of a camera is installed." Hiroshi, Claim 10. A POSITA would have understood that Hiroishi's program would be alternative term for the mobile software application. A POSITA would have understood that the mobile phone 40 would have implemented the mobile software application to execute the program (or set of instructions).

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

[12.2] establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein paired secure Bluetooth connection uses cryptographic encryption key;

304. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.2] per the Bluetooth specification. In my opinion, Hiroishi-Kahn-Bluetooth teaches establishing a paired secure connection between the Bluetooth enabled mobile

device and a Bluetooth enabled data capture device, wherein the paired secure Bluetooth connection uses cryptographic encryption key. For example, Hiroishi discloses "photographing system 10 …is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth… and can perform transfer of data signals." Hiroishi, [0066]-[0067]. The connection is paired because it allows two-way communication between the digital camera 50 and cellular phone 40. Id., [0066]. In FIG. 5, Hiroishi illustrates remote control of the digital camera by the cellular phone. Hiroishi, FIG. 5, [0071]-[0078]. In steps 100 and 104, the camera determines whether it is under remote control of the phone via the Bluetooth connection. Id. See also, Hiroishi, [0070], [0074]-[0088], [0091]-[0107], [0121].

305. To the extent the Patent argues that Hiroishi does not expressly disclose that the Bluetooth pairing between the cellular phone and the digital camera includes using a cryptographic encryption key, it would have been obvious to a POSITA to modify Hiroishi to include this limitation. The use of such cryptographic encryption keys was a standard and well known part of the Bluetooth specification. For example, as discussed in the Bluetooth Core Specification V2.1, pairing between Bluetooth devices includes the generation and exchange of initialization keys created from a PIN, a random number, and a Bluetooth Device Address (BD_ADDR):

306. Referring to Bluetooth Core Specification 2.1 (July 2007),

4.2.2 Pairing

When two devices do not have a common link key an initialization key (K_{init}) shall be created based on a PIN, and a random number and a BD_ADDR. K_{init} shall be created as specified in [Part H] Section 6.3 on page 805. When both devices have calculated K_{init} the link key shall be created, and a mutual authentication is performed. The pairing procedure starts with a device sending an LMP_in_rand PDU; this device is referred to as the "initiating LM" or "initiator" in Section 4.2.2.1 on page 251 - Section 4.2.2.5 on page 253. The other device is referred to as the "responding LM" or "responder". The PDUs used in the pairing procedure are:

M/O	PDU	Contents
M	LMP_in_rand	random number
M	LMP_au_rand	random number
M	LMP_sres	authentication response
M	LMP_comb_key	random number
M	LMP_unit_key	key

Table 4.13: PDUs used for pairing

All sequences described in Section 4 on page 233, including the mutual authentication after the link key has been created, shall form a single transaction. The transaction ID from the first LMP_in_rand shall be used for all subsequent sequences.

See, e.g., Bluetooth Specification V2.1, 412.

1 SECURITY OVERVIEW

Bluetooth wireless technology provides peer-to-peer communications over short distances. In order to provide usage protection and information confidentiality, the system provides security measures both at the application layer and the link layer. These measures are designed to be appropriate for a peer environment. This means that in each device, the authentication and encryption routines are implemented in the same way. Four different entities are used for maintaining security at the link layer: a Bluetooth device address, two secret keys, and a pseudo-random number that shall be regenerated for each new transaction. The four entities and their sizes are summarized in Table 1.1.

Entity	Size
BD_ADDR	48 bits
Private user key, authentication	128 bits
Private user key, encryption configurable length (byte-wise)	8-128 bits
RAND	128 bits

Table 1.1: Entities used in authentication and encryption procedures.

The Bluetooth device address (BD_ADDR) is the 48-bit address. The BD_ADDR can be obtained via user interactions, or, automatically, via an inquiry routine by a device.

The secret keys are derived during initialization and are never disclosed. The encryption key is derived from the authentication key during the authentication process. For the authentication algorithm, the size of the key used is always 128 bits. For the encryption algorithm, the key size may vary between 1 and 16 octets (8 - 128 bits). The size of the encryption key is configurable for two reasons. The first has to do with the many different requirements imposed on cryptographic algorithms in different countries – both with respect to export regulations and official attitudes towards privacy in general. The second reason is to facilitate a future upgrade path for the security without the need of a costly redesign of the algorithms and encryption hardware; increasing the effective key size is the simplest way to combat increased computing power at the opponent side.

See, e.g., Bluetooth Specification V2.1, 1025.

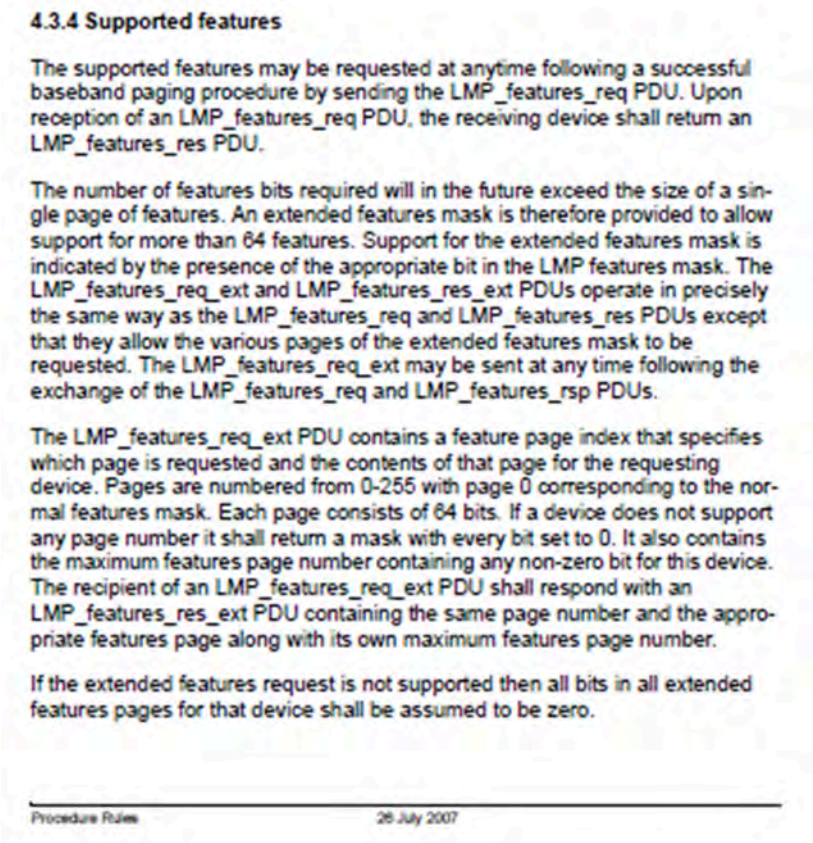
307. Cryptographic authentication between wireless devices like a digital camera and cellular phone was routine at the time of the invention. Indeed, cryptographic authentication was part of the Bluetooth standard for years before the alleged Critical Date of the '030 Patent.

308. A POSITA would have understood the basic motivation for using cryptographic authentication: to ensure that each device is communicating with its intended recipient and that information is protected from outsiders when transmitted between devices. A POSITA would have found this benefit directly applicable to the system disclosed Hiroishi, because it would have ensured the secure transmission of image files and related data between the two devices. Hiroishi teaches that the camera and phone implement a "predetermined communication protocol" and identifies Bluetooth as the preferred data transmission mechanism, so there would not have been any unexpected result if the camera and phone were configured to cryptographically authenticate each other.

[12.3] receiving a message from the Bluetooth enabled data capture device, corresponding to supported data capability of the Bluetooth enabled data capture device;

309. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.3] per the Bluetooth specification. In my opinion, Hiroishi-Kahn-Bluetooth teaches that the software module on the Bluetooth enabled mobile device is configured to perform the step of receiving a message (LMP_features_res) from the Bluetooth

enabled data capture device (Hiroishi's digital camera 50), corresponding to supported data capability of the Bluetooth enabled data capture device. Indeed, a POSITA would have recognized that Hiroishi's Bluetooth communication between the mobile phone 40 and the digital camera 50 complies with the Bluetooth protocols available in 2007 which required the exchange of supported features between the Bluetooth devices. See Bluetooth Section 4.3.4 (shown below).



4.3.4 Supported features

The supported features may be requested at anytime following a successful baseband paging procedure by sending the LMP_features_req PDU. Upon reception of an LMP_features_req PDU, the receiving device shall return an LMP_features_res PDU.

The number of features bits required will in the future exceed the size of a single page of features. An extended features mask is therefore provided to allow support for more than 64 features. Support for the extended features mask is indicated by the presence of the appropriate bit in the LMP features mask. The LMP_features_req_ext and LMP_features_res_ext PDUs operate in precisely the same way as the LMP_features_req and LMP_features_res PDUs except that they allow the various pages of the extended features mask to be requested. The LMP_features_req_ext may be sent at any time following the exchange of the LMP_features_req and LMP_features_rsp PDUs.

The LMP_features_req_ext PDU contains a feature page index that specifies which page is requested and the contents of that page for the requesting device. Pages are numbered from 0-255 with page 0 corresponding to the normal features mask. Each page consists of 64 bits. If a device does not support any page number it shall return a mask with every bit set to 0. It also contains the maximum features page number containing any non-zero bit for this device. The recipient of an LMP_features_req_ext PDU shall respond with an LMP_features_res_ext PDU containing the same page number and the appropriate features page along with its own maximum features page number.

If the extended features request is not supported then all bits in all extended features pages for that device shall be assumed to be zero.

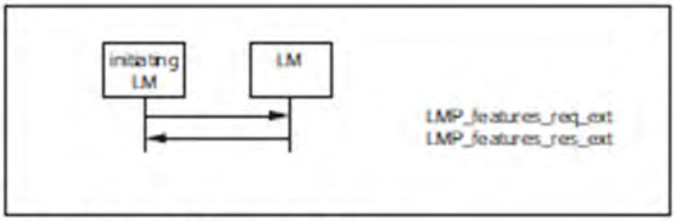
Procedure Rules 26 July 2007

M/O	PDU	Contents
M	LMP_features_req	features
M	LMP_features_res	features
O(63)	LMP_features_req_ext	features page max supported page extended features
O(63)	LMP_features_res_ext	features page max supported page extended features

Table 4.22: PDUs used for features request.



Sequence 68: Request for supported features.



Sequence 69: Request for extended features.

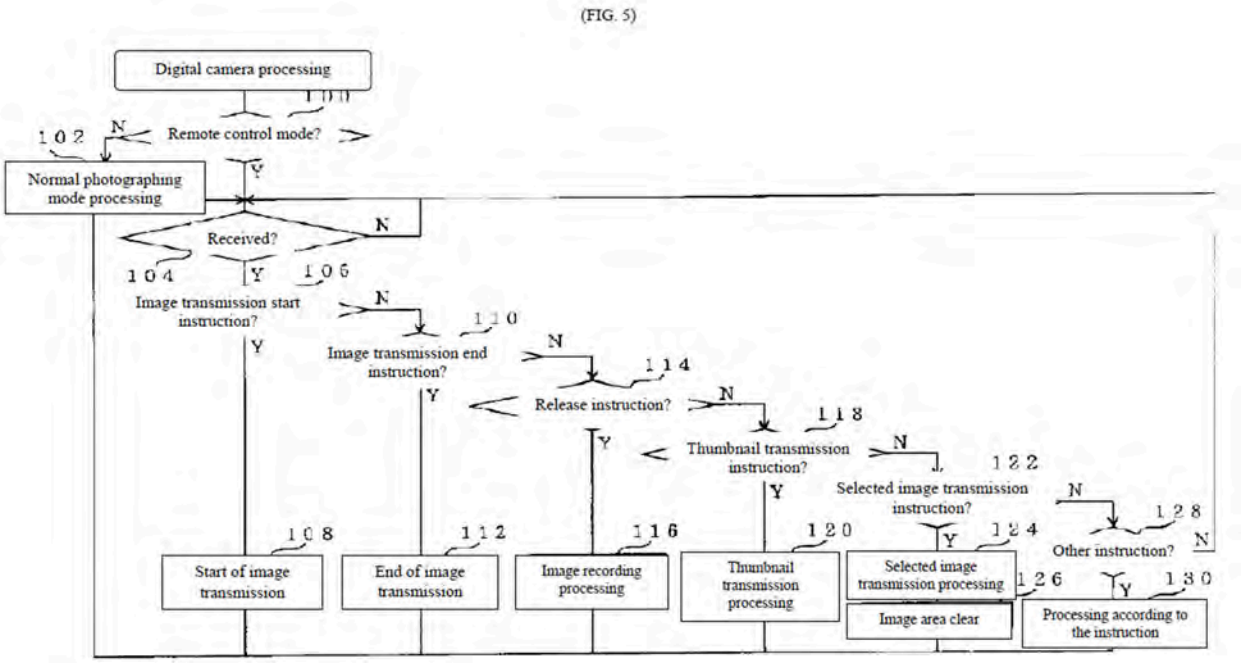
310. As shown above, the ***max supported page*** is indicative of supported data capability of the Bluetooth enabled mobile device. Other examples of features that are reported include number of slots per packet (3 slot packets or 5 slot packets), Adaptive Frequency Hopping (AFH) capability, Channel Quality Driven Data Rate, and Enhanced Data Rate (EDR). Bluetooth Core Specification V2.1, 384-387 (explaining feature definitions).

311. A POSITA would have found is obvious that that in order to receive a message from a Bluetooth-enabled data capture device, it is essential to match the

supported data capability of the Bluetooth-enabled device. This alignment ensures the effective establishment of communication between a mobile phone and a digital camera, thereby facilitating superior data transmission in accordance with the Bluetooth standard.

[12.4] detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:

312. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.4]. In my opinion, Hiroishi-Kahn-Bluetooth teaches detecting new data acquired by the Bluetooth enabled data capture device for transfer. For example, Hiroishi teaches detection of new-data by sending a "release instruction" from the cellular phone 40 to the digital camera 50 after establishing a Bluetooth connection between the camera and the phone. Hiroishi, Abstract, [0012]. Hiroishi emphasizes that "the release instruction information is the information for instructing the timing of photographing with the camera of the present invention." Hiroishi, [0034]. The release instructions from the mobile phone would allow the camera "to photograph a picture… by transmitting the release instruction information at the timing one wishes to take a photograph with the camera of the present invention. Therefore, since the timing in which the release instruction information is transmitted serves as the photographing timing, the photographer can grasp the photographing timing correctly." Id., [0034].



Hiroishi, FIG. 5.

313. As shown above in FIG. 5, Hiroishi illustrates remote control of the digital camera by the cellular phone. Hiroishi, FIG. 5, [0071]-[0078]. In steps 100 and 104, the camera determines whether it is under remote control of the phone via the Bluetooth. *Id*. At step 114, the camera receives a release instruction from the phone causing it to acquire a new image. *Id*., Abstract ("the mobile phone 40… transmits the release instruction information to the digital camera 50"), [0034] ("it is possible to photograph a picture with a camera also at the position away from the camera, by transmitting the release instruction information at the timing one wishes to take a photograph with the camera"), [0078] ("In Step 114, a determination is made as to whether the instruction information received in Step 104 is the release instruction information…."). A POSITA would understand that,

because the release instruction is received from the phone over the Bluetooth connection, the image is acquired after the wireless connection is established. *Id*.

314. In summary, a POSITA would have understood that Hiroishi detects new data acquired because when 1) the user sends a "release instruction" to the camera, resulting in the camera storing a captured image in its memory; 2) the user instructs the camera to end image transmissions; 3) the camera generates thumbnail images of the images stored in memory; and 4) the cellular phone receives the thumbnail images. The reception of the thumbnail images is the **detection** of new-data acquired. (emphasis added)

[12.5] sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data,
wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;

315. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.5]. In my opinion, Hiroishi-Kahn-Bluetooth teaches that the detecting step (see Element [12.4]) includes sending a message (Hiroishi's thumbnail transmission instruction) to the Bluetooth enabled data capture device (Hiroishi's digital camera 50), over the established paired secure Bluetooth connection, to enable event notifications (Hiroishi's thumbnail images) on the Bluetooth enabled data capture device corresponding to new data (full resolution photographs), wherein the new data is

data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device (mobile phone 40). This limitation is broken down into constituent steps below:

[12.5.1] sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data,

316. For example, Hiroishi teaches sending a message (thumbnail transmission instruction) to the Bluetooth enabled camera to enable event notifications (thumbnail images). The mobile phone sends an instruction to the camera to transmit thumbnail images of the captured images stored on the camera's memory. Supra [12.4]. Specifically, Hiroishi teaches the following instructions that are sent from the mobile phone to the camera. Hiroishi, [0068] ("Image transmission end instruction information ... is the information for instructing the stop of the transmission of the digital image data started according to the image transmission start instruction information ... 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.") Hiroishi discloses that after the mobile phone sends a thumbnail transmission instruction to the camera, the camera processes images stored in memory (i.e., the new data) to create thumbnails, and

sends the thumbnails to the mobile phone. TTI-1011, [0081].

317. Hiroishi discloses that after, "the instruction information received . . . image data that can display thumbnails is created by performing a predetermined image processing to the digital image data stored in the photographed image data storage area of SDRAM 55A (not shown), a thumbnail transmission processing for transmitting the image data to the mobile phone 40 is performed, and the process returns to Step 104 thereafter…image processing performed here is as follows: the graphical data compression/ decompression unit 62 decompresses all the compressed digital image data stored in SDRAM 55A, the image data is thinned at a predetermined thinning rate, the digital image data obtained thereby is used to create the image data with which thumbnails can be displayed, and the image data is compressed again by the graphical data compression/ decompression unit 62. Thereby, the size of the image data that can display thumbnails to be transmitted to the mobile phone 40 can be made small, enabling high-speed transmission" Id., [0081]-[0082]. Then, the thumbnails are "transmitted according to the thumbnail transmission instruction information" to the mobile phone 40., Hiroishi, [0067], [0084].

318. Thus, the mobile phone sends the camera a thumbnail transmission instruction, which is a message to enable event notifications corresponding to the new data. The full resolution images stored in memory are the "new data," and

therefore, the thumbnails are notifications of the capture of the new data. Likewise, the thumbnails "correspond" to the new data because the thumbnails are a lower resolution representation of the full resolution captured images stored in memory on the camera.

[12.5.2] wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;

319. Because the new data (full resolution image) is obtained in response to instructions received by the digital camera 50 from the mobile phone 40 over the Bluetooth connection, the new data is acquired by the Bluetooth enabled data capture device (digital camera 50) after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device (digital camera 50) and the Bluetooth enabled mobile device (mobile phone 40).

320. Hiroishi teaches that the mobile phone 40 and the digital camera 50 are connected by a Bluetooth connection. Hiroishi, [0066] ("The photographing system 10 according to this embodiment is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth."), [0067] ("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. In this embodiment, the communication unit 49 is built in the mobile phone 40,

and the communication unit 59 is built in the digital camera 50"), [0121] ("In this embodiment, the case where Bluetooth is applied as a standard of communication for the communication unit 49 and the communication unit 59 has been described . . . "). Further, Hiroishi discusses all of the instructions transmitted to and images received from the camera. *See, e.g*., Hiroishi, [0073]-[0088], see also, e.g., id., [0091]-[0107], [0121].

[12.6] enabling event notification listening on Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;

321. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.6]. In my opinion, Hiroishi-Kahn-Bluetooth teaches that the detecting step (*see* Element [12.4]) includes enabling event notification listening (activating the mobile phone code that "waits" to receive thumbnail images from the camera) on Bluetooth enabled mobile device, to listen ("wait") for event notifications (thumbnail images) sent from the Bluetooth enabled data capture device (digital camera 50), over the established paired secure Bluetooth connection. As discussed above (see supra [12.4]), after the mobile phone sends a thumbnail transmission instruction to the camera, the mobile phone "waits" to receive the thumbnails from the camera. A POSITA would recognize this "waiting" is the mobile phone listening for the event notifications (the thumbnails). Hiroishi, [0102] ("If yes in Step 222, that is, when the operator has specified the transmission of the image transmission end

instruction information, the process goes to Step 226, wherein the image transmission end instruction information is transmitted via the communication unit 49 to the digital camera 50, and the thumbnail transmission instruction information is subsequently transmitted via the communication unit 49 to the digital camera 50 in Step 228. In response thereto, the digital camera 50 stops the image transmission processing performed in Step 112 of the digital camera processing described above, the thumbnail transmission processing is subsequently performed in Step 120, and the image data for displaying thumbnails is transmitted to the mobile phone 40."), [0104] ("In the following Step 230, [the phone] **waits** until it receives the image data that can display the thumbnail from the digital camera 50 . . . .") (emphasis added).

322. This "waiting" is the mobile phone listening for event notifications. A POSITA would understand that the term "waiting" (in step 230) in the context of the mobile phone's action after sending a thumbnail transmission instruction to the camera implies a state where the mobile phone is actively listening for event notifications, particularly for the receipt of thumbnails from the camera. This interpretation aligns with the typical operation of communication systems, where devices often enter a state of waiting or listening for incoming data or signals. In the described scenario, the mobile phone activates and remains in a listening state until it receives the image data necessary to display thumbnails from the digital

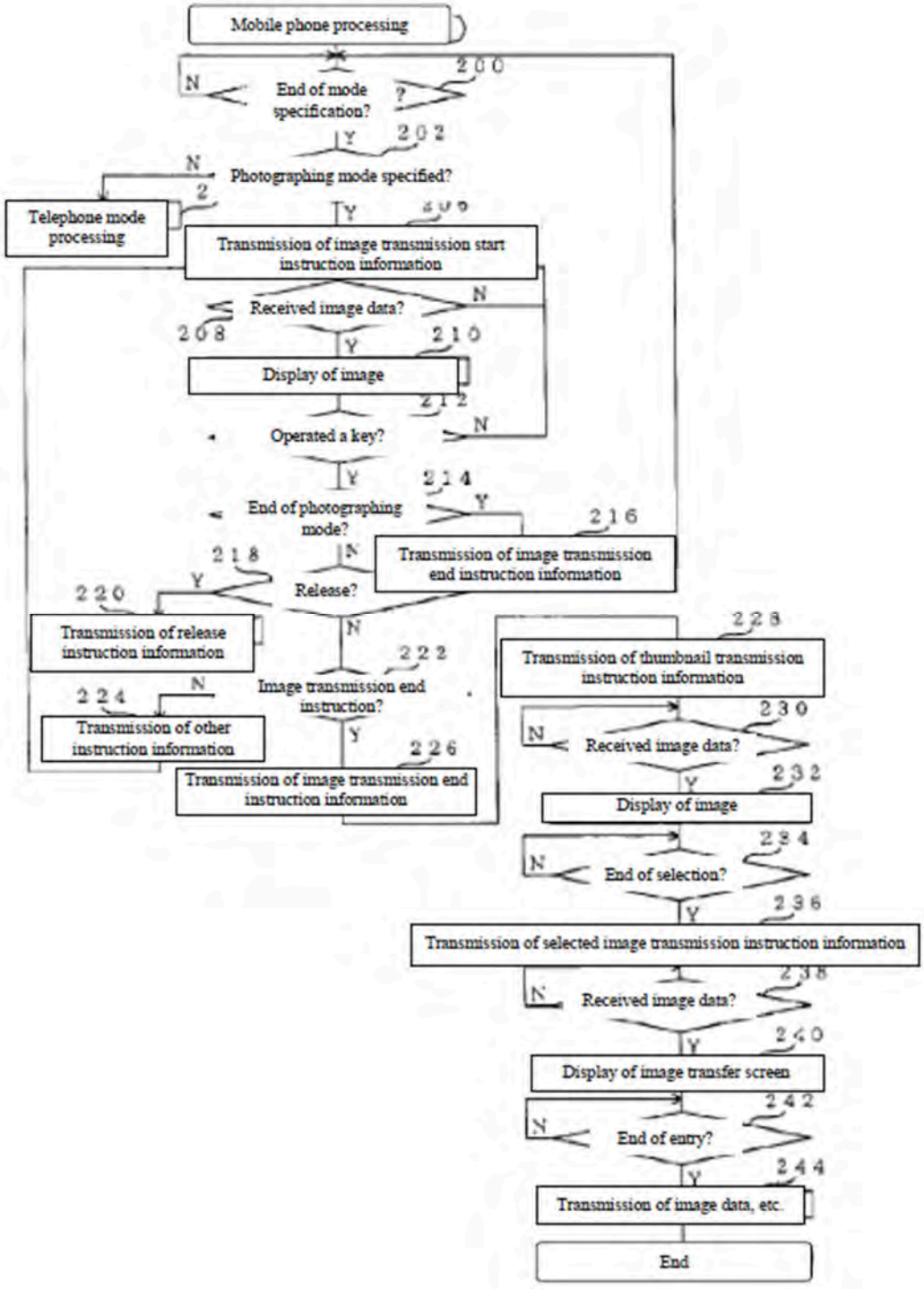
camera. This waiting period serves as a mechanism for the mobile phone to remain responsive to event notifications and effectively manage the data transmission process between itself and the camera. Such listening behaviors are common across various elements in similar patents within the domain, reflecting the standard practices and expectations within the field of communication protocols and device interaction.

[12.7] receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and

323. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.7]. In my opinion, Hiroishi-Kahn-Bluetooth teaches receiving, from the Bluetooth enabled data capture device, an event notification (thumbnail image) corresponding to existence of new data (full-resolution image) for transfer, over the established paired secure Bluetooth connection. For example, Hiroishi teaches "[a] recording medium, capable of being read by a computer in which a program that controls the operation of a camera is installed." Hiroshi, Claim 10. A POSITA would have understood that Hiroishi's program would be alternative term for the mobile software application. The program (mobile software application) is configured to wait for response (listen) for a thumbnail image (an event notification) from the camera over the Bluetooth connection, as shown in Fig. 6, the loop until the entire thumbnail is received in step 230, wherein the thumbnail

(event notification) is the lower resolution image corresponding to the acquired full resolution image (new-data) and comprises sending a thumbnail over Bluetooth connection from the camera to the phone. Hiroishi, [0081]-[0082], [0104]-[0105]. A POSITA would have understood that the phone's (and/or program installed on the phone. Hiroishi, Claim 10, Abstract) "wait" action for the thumbnail images, constitutes as the phone listening for the event notification signal. See also, Supra [12.4].

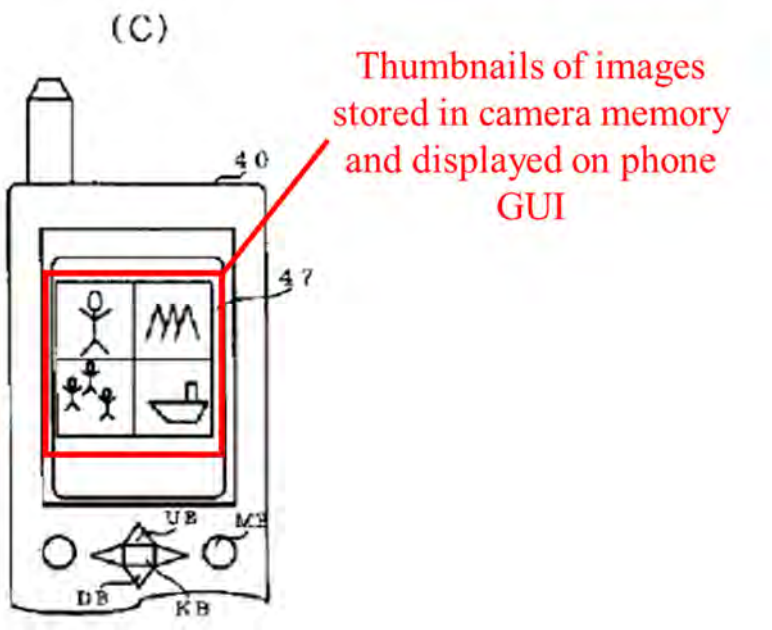
(FIG. 6)



Hiroishi, FIG. 6.

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

to the digital camera, the cellular phone "waits" for the image data in response. Hiroishi, [0102]-[0104]. Subsequently, the camera performs "thumbnail transmission… and the image data for displaying thumbnails is transmitted to the mobile phone 40." Hiroishi, [0102]. During this time, the phone "waits until it receives the image data that can display the thumbnail from the digital camera 50, and in the following Step 232, after a decompression process is performed to the received image data, the thumbnail shown according to the image data is displayed on the display unit 47 [of the phone]." Hiroishi, [0104].



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

325. The thumbnails correspond to the acquired new data (the image captured by the camera when the release instruction is given). The "image data that can display thumbnails is created by performing a predetermined image

processing to the digital image data stored in the photographed image data storage area of SDRAM 55A (not shown), a thumbnail transmission processing for transmitting the image data to the mobile phone 40 is performed, and the process returns to Step 104 thereafter." Hiroishi, [0081]-[0082]; *see also* claim 10, [0066]-[0068], [0121].

326. A POSITA would have also understood that the thumbnails being sent to the phone from the camera constitute the event notification.

[12.8] sending a request to the Bluetooth enabled data capture device, to get new data for transfer;

327. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.8]. In my opinion, Hiroishi-Kahn-Bluetooth teaches sending a request (Hiroishi's "selected image transmission instruction") to the Bluetooth enabled data capture device (digital camera 50), to get new data (full resolution images) for transfer from Hiroishi's digital camera 50 to Hiroishi's mobile phone 40. Hiroishi teaches that the user of the mobile phone can select thumbnail images the user wants to receive from the camera. The selection of the images is an instruction sent to the camera for the camera to retrieve the images from memory, process the images, and send the images back to the mobile phone. Hiroishi, [0068] ("Selected image transmission instruction information ... is the information for instructing the transmission of the [full resolution] digital image data corresponding to the image chosen from the [lower resolution] image shown by the thumbnails transmitted

according to the thumbnail transmission instruction information by the operator of the mobile phone 40.") A POSITA would have recognized that selected image transmission instruction is the request to get new data for transfer.

[12.9] receiving, by the Bluetooth enabled mobile device, encrypted data corresponding to the new data over the established Bluetooth paired secure wireless connection and obtaining new data from the received encrypted data using cryptographic encryption key; and

328. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.9]. In my opinion, Hiroishi-Kahn-Bluetooth teaches receiving, by the Bluetooth enabled mobile device, encrypted data corresponding to the new data over the established Bluetooth paired secure wireless connection and obtaining new data from the received encrypted data using cryptographic encryption key. For example, Hiroishi teaches that the new data (captured images stored in camera memory) are received by the mobile phone in response to the selection of thumbnails.

> Once the thumbnails are displayed on the display unit 47, an operator presses the UB, DB, or KB key provided on the mobile phone 40 to select a desired image (the image [the operator] desires to request a print shop to make prints (also see FIG. 2) or the image for which [the operator] desires to transmit the digital image data to a terminal unit 22 installed at home or a terminal unit 24 installed at a friend's house) from the thumbnails.
>
> Then, in the following Step 234, [the phone] waits for the end of selection of the desired image requested by the operator, and in the following Step 236, the information that can specify the image selected by the operator and the selected image transmission instruction information are transmitted to the digital camera 50 via the communication

> unit 49. **In response thereto, the digital camera 50 transmits to the mobile phone 40 the digital image data corresponding to the image selected** by the operator by performing the selected image transmission processing in the above described Step 124 of the digital camera processing, and then the digital image data corresponding to the image chosen by the operator in Step 126 is deleted from SDRAM 55A.
>
> In the following Step 238, [the phone] waits for the reception of the digital image data transmitted from the digital camera 50, and in the following Step 240, a predetermined image transfer screen is displayed on the display unit 47.

Hiroishi, [0105]-[0107] (emphasis added).

329. A POSITA would have found it obvious in view of the Bluetooth specification that encrypting the new data captured by the camera before transmission to the mobile phone offers numerous benefits, primarily ensuring the integrity and security of the data during transfer. Encryption provides a safeguard against potential eavesdropping and unauthorized access, thereby preserving the confidentiality of sensitive information, such as captured images.

330. Furthermore, a POSITA would have had a reasonable expectation of success in implementing encryption for data transmission between the camera and the mobile phone. The Bluetooth specification provides comprehensive details and guidelines on how to incorporate encryption mechanisms into communication protocols between Bluetooth-enabled devices. With readily available information and resources regarding encryption techniques within the Bluetooth framework, a

POSITA would anticipate achieving successful implementation without encountering insurmountable challenges.

331. Moreover, it was commonplace within the field for devices to perform encryption on transmitted data to ensure secure communication channels. This established practice underscores the familiarity and feasibility of integrating encryption mechanisms into the data transmission process between the camera and the mobile phone. Once data is encrypted for transmission, decryption becomes a necessary counterpart to ensure that the recipient device can access and utilize the transmitted information. The Bluetooth specification also offers detailed insights into how to perform decryption, thereby enabling a POSITA to effectively implement the decryption process on the receiving end.

332. In summary, considering the benefits of encryption, the readily available information within the Bluetooth specification regarding encryption and decryption techniques, and the common practice of securing data transmission through encryption, it would have been obvious to a POSITA to employ Bluetooth encryption for protecting the integrity and confidentiality of the data transferred from the camera to the mobile phone, as well as to implement decryption for accessing the encrypted data on the receiving device.

7 BITSTREAM PROCESSING

Bluetooth devices shall use the bitstream processing schemes as defined in the following sections.

Before the payload is sent over the air interface, several bit manipulations are performed in the transmitter to increase reliability and security. An HEC is added to the packet header, the header bits are scrambled with a whitening word, and FEC coding is applied. In the receiver, the inverse processes are carried out. Figure 7.1 on page 129 shows the processes carried out for the packet header both at the transmit and the receive side. All header bit processes are mandatory.

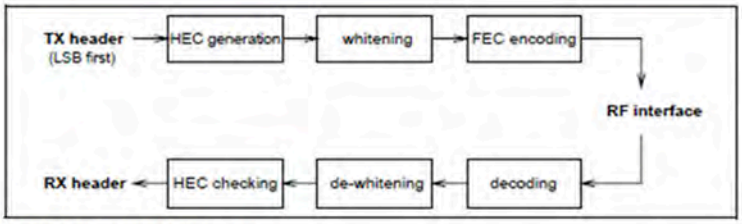


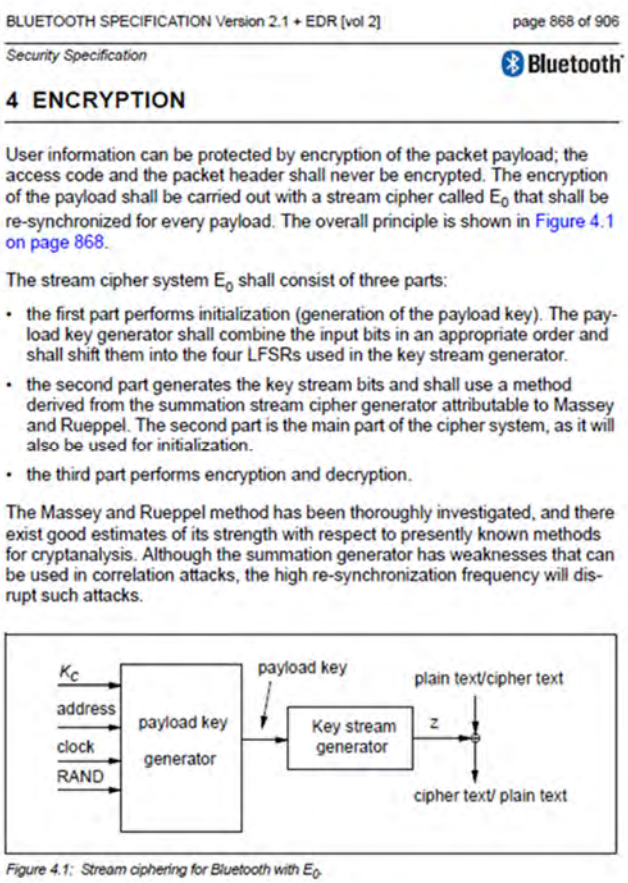
Figure 7.1: Header bit processes.

Figure 7.2 on page 129 shows the processes that may be carried out on the payload. In addition to the processes defined for the packet header, encryption can be applied on the payload. Only whitening and de-whitening, as explained in Section 7.2 on page 133, are mandatory for every payload; all other processes are optional and depend on the packet type (see Section 6.6 on page 121) and whether encryption is enabled. In Figure 7.2 on page 129, optional processes are indicated by dashed blocks.



Figure 7.2: Payload bit processes.

Bluetooth Core Specification V2.1, 299



BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 2] page 868 of 906

Security Specification

Bluetooth

4 ENCRYPTION

User information can be protected by encryption of the packet payload; the access code and the packet header shall never be encrypted. The encryption of the payload shall be carried out with a stream cipher called E_0 that shall be re-synchronized for every payload. The overall principle is shown in Figure 4.1 on page 868.

The stream cipher system E_0 shall consist of three parts:

- the first part performs initialization (generation of the payload key). The payload key generator shall combine the input bits in an appropriate order and shall shift them into the four LFSRs used in the key stream generator.
- the second part generates the key stream bits and shall use a method derived from the summation stream cipher generator attributable to Massey and Rueppel. The second part is the main part of the cipher system, as it will also be used for initialization.
- the third part performs encryption and decryption.

The Massey and Rueppel method has been thoroughly investigated, and there exist good estimates of its strength with respect to presently known methods for cryptanalysis. Although the summation generator has weaknesses that can be used in correlation attacks, the high re-synchronization frequency will disrupt such attacks.

Figure 4.1: Stream ciphering for Bluetooth with E_0.

Bluetooth Core Specification V2.1, 1038

[12.10] transferring the obtained new data along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server,
wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.

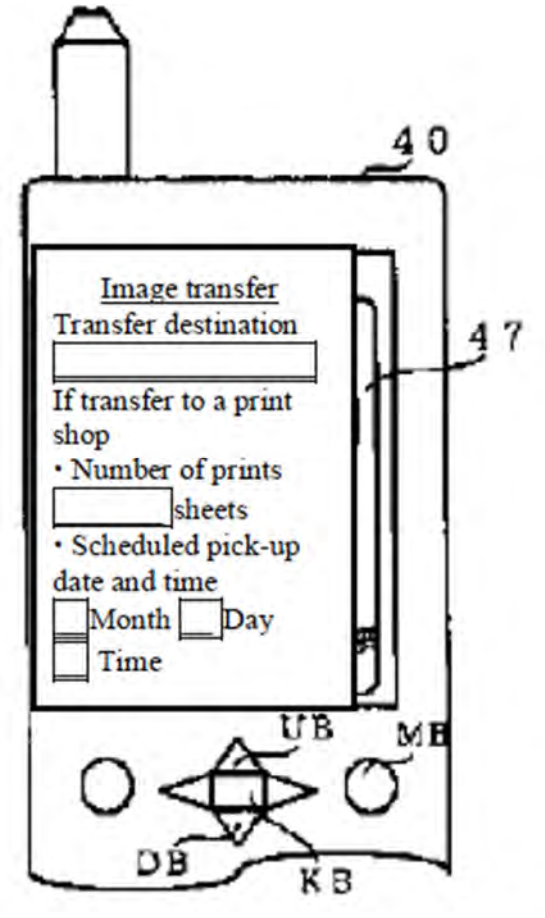
333. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.10].

In my opinion, Hiroishi-Kahn-Bluetooth teaches transferring the obtained new data along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a

remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server. This limitation is broken down into constituent steps below:

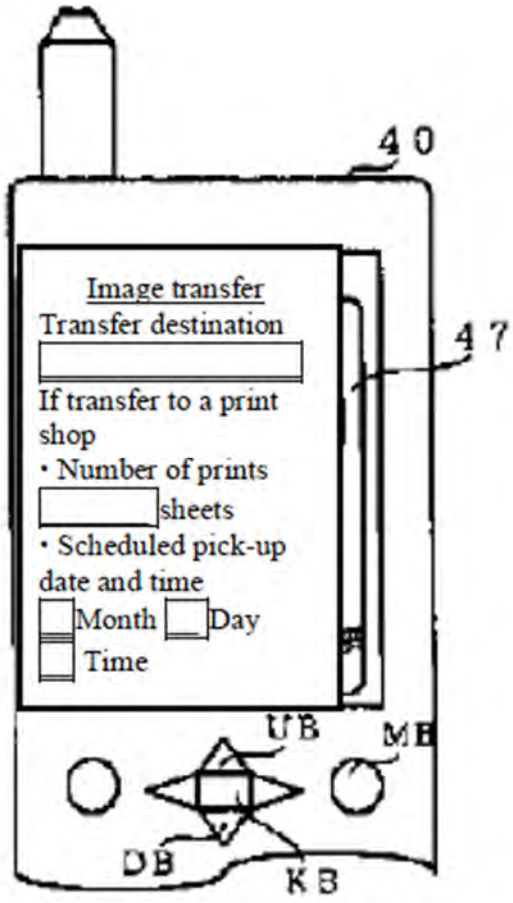
[12.10.1] transferring the obtained new data along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and

334. As discussed above, Hiroishi establishes that the mobile phone is configured to communicate with one or more remote servers using a wireless phone network. Hiroishi teaches sending the images to a remote terminal, such as a terminal device at a friend's house, the user's house, or a print shop. *See, e.g.*, Hiroishi, FIG. 2. Hiroishi teaches configuring the obtained new data with a destination web address. In Hiroishi, the email address of the remote terminal is used for uploading the images to the remote terminal. E.g., Hiroishi, [0110], FIG. 7(D).



Hiroishi, FIG. 7(D).

335. Hiroishi teaches configuring the obtained new data to comprise an action setting, which I understand to include commands by the user. E.g., from infringement claim chart, the "uploaded data includes the command provided by the user such as 'like' or 'scroll down.'" The action setting of Hiroishi includes user instructions for a number of sheets for printing and a schedule pick-up date and time. E.g., Hiroishi, FIG. 7D.



Hiroishi, FIG. 7D

336. Hiroishi is silent as to the action setting comprising a RPC or HTTP method. However, a POSITA would have found it obvious to use HTTP methods for an action setting. Given the widespread use of HTTP, a POSITA would have understood that Hiroishi's mobile phone would have implemented communication with network 12 using HTTP.

337. In my opinion, Kahn teaches these limitations. For example, Kahn discloses that, "to communicate with the image management server 330, the host device 320 establishes an Internet connection to the server, for example, using

HTTP protocol." TTI-1017, [0056]. A POSITA would have found it obvious to use HTTP methods for an action setting as taught by Kahn. For example, Kahn is directed to wirelessly transferring image files from a mobile device to a publishing website over the Internet with an HTTP action setting. *See, e.g.*, Kahn, [0056], [0077] (describing the action setting of creating a new album on the server for uploading the images). A POSITA would have been motivated to implement teachings of Kahn in Hiroishi's mobile phone to have communication with network 12 using HTTP. Specifically, it would have been obvious for Hiroishi's phone application to use HTTP (webmail) to transfer the received new-data (full resolution image) along with a user authentication credential (email address of the sender/phone application user) to a remote server (e.g., an email server hosting the email address of the terminal unit of the transfer destination) over a cellular data network (Hiroishi's cellular data network).

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

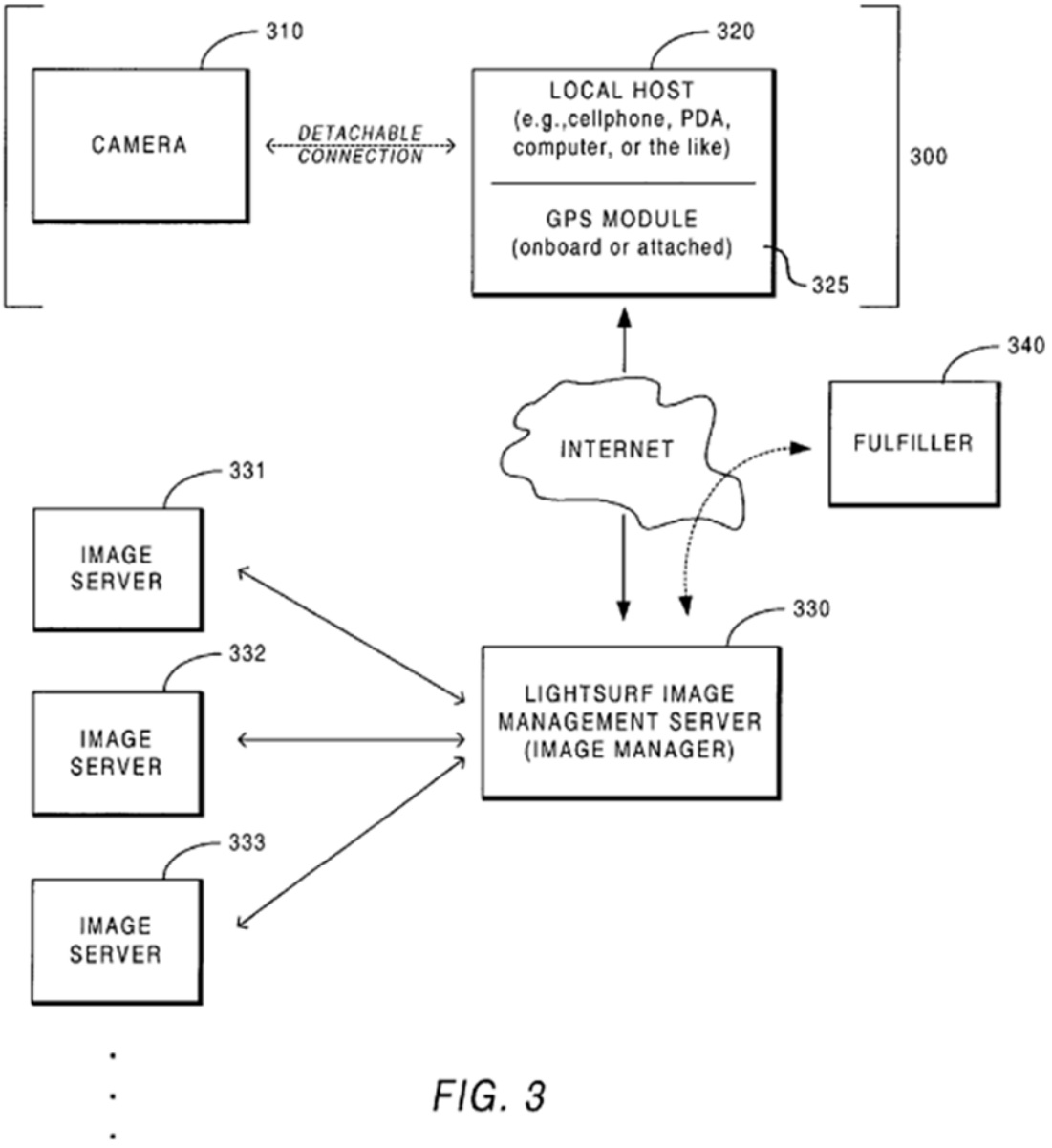


FIG. 3

Kahn, FIG. 3.

[12.10.2] wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.

339. A POSITA would have found it obvious to also include an email address or other identification information for the operator of the mobile phone with the images sent to the remote server, such as the print shop, so that images

could be associated with the operator. Even though Hiroishi discusses using caller ID to authenticate the operator when collecting the printouts, a POSITA would have recognized that the photographic system would have benefited from some identifying information associated with the images when they are transferred to the remote server. Otherwise, how would the print shop know which images belong to which operator. After the images are identified as being for the operator, the operator can then be authenticated using the caller ID.

340. For example, in the same field of endeavor, Kahn teaches "transmitting the images from the imaging device to a corresponding user account on a Web server." Kahn, Claim 12. Also, Kahn, [0057] ("The user employs the camera 310 to take various pictures (i.e., capture images). Immediately or at some convenient point in time, location ID information (i.e., GPS information) from the GPS module 325 is associated with the images that are captured. The images are ultimately uploaded to a corresponding user account at the image management server 330. In the currently preferred embodiment, the 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.")

[15.P] A method for transferring data to a remoter internet server by a Bluetooth enabled mobile device comprising:

341. To the extent the preamble is limiting, the Hiroishi-Kahn-Bluetooth

combination renders obvious [15.P]. In my opinion, Hiroishi-Kahn-Bluetooth teaches a method for transferring data to a remoter internet server by a Bluetooth enabled mobile device. Supra [12.P].

[15.1] performing at a Bluetooth enabled mobile device:

342. The Hiroishi-Kahn-Bluetooth combination renders obvious [15.1]. In my opinion, Hiroishi-Kahn-Bluetooth teaches performing at a Bluetooth enabled mobile device. Supra [12.1].

[15.2] establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein the secure paired Bluetooth connection uses cryptographic encryption key;

343. The Hiroishi-Kahn-Bluetooth combination renders obvious [15.2]. In my opinion, Hiroishi-Kahn-Bluetooth teaches establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein the secure paired Bluetooth connection uses cryptographic encryption key. Supra [12.2].

[15.3] detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:

344. The Hiroishi-Kahn-Bluetooth combination renders obvious [15.3]. In my opinion, Hiroishi-Kahn-Bluetooth teaches detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer. Supra [12.4].

[15.4] sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;

345. The Hiroishi-Kahn-Bluetooth combination renders obvious [15.4]. In my opinion, Hiroishi-Kahn-Bluetooth teaches sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device. Supra [12.5].

[15.5] enabling event notification listening on the Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;

346. The Hiroishi-Kahn-Bluetooth combination renders obvious [15.5]. In my opinion, Hiroishi-Kahn-Bluetooth teaches enabling event notification listening on the Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection. Supra [12.6].

[15.6] receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and

347. The Hiroishi-Kahn-Bluetooth combination renders obvious [15.6]. In my opinion, Hiroishi-Kahn-Bluetooth teaches receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection. Supra [12.7].

[15.7] sending a request to the Bluetooth enabled data capture device, to get new data object for transfer,
wherein new data object comprises of new data, data associated with new data and time-stamp, and
wherein the time-stamp corresponds to a time when new data was acquired;

348. The Hiroishi-Kahn-Bluetooth combination renders obvious [15.7]. In my opinion, Hiroishi-Kahn-Bluetooth teaches sending a request to the Bluetooth enabled data capture device, to get new data object for transfer, wherein new data object comprises of new data, data associated with new data and time-stamp, and wherein the time-stamp corresponds to a time when new data was acquired. Supra [12.8]. Kahn explains that "prior art imaging devices have…been able to record information about the date/time (timestamp) that an image was captured". TTI-1017, [0008].

[15.8] receiving, by the Bluetooth enabled mobile device, encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection;

349. The Hiroishi-Kahn-Bluetooth combination renders obvious [15.8]. In

my opinion, Hiroishi-Kahn-Bluetooth teaches receiving, by the Bluetooth enabled mobile device, encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection. Supra [12.9].

[15.9] obtaining new data, data associated with new data and time-stamp from the received encrypted data object using cryptographic encryption key; and

350. The Hiroishi-Kahn-Bluetooth combination renders obvious [15.9]. In my opinion, Hiroishi-Kahn-Bluetooth teaches obtaining new data, data associated with new data and time-stamp from the received encrypted data object using cryptographic encryption key. For example, Kahn teaches that "the image data already includes timestamp information (i.e., timestamp indicating when the image is captured)". TTI-1017, [0050]. As I described in [12.9], in the Hiroishi-Kahn-Bluetooth system, the new data picture received by the mobile device is encrypted. Supra [12.9].

[15.10] sending the obtained new data and the obtained time-stamp along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server,
wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.

351. The Hiroishi-Kahn-Bluetooth combination renders obvious [15.10]. In my opinion, Hiroishi-Kahn-Bluetooth teaches sending the obtained new data and the obtained time-stamp along with a user identifier to a remote internet server,

comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server. Supra [12.10].

[1.P] A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:

352. To the extent the preamble is limiting, the Hiroishi-Kahn-Bluetooth combination renders obvious [1.P]. In my opinion, Hiroishi-Kahn-Bluetooth teaches a method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device. Supra [12.P].

[1.1] performing at a Bluetooth enabled data capture device:

353. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.1]. In my opinion, Hiroishi-Kahn-Bluetooth teaches performing at a Bluetooth enabled data capture device. Supra [12.1].

[1.2] establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;

354. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.2]. In

my opinion, Hiroishi-Kahn-Bluetooth teaches 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. Supra [12.2].

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

355. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.3]. In my opinion, Hiroishi-Kahn-Bluetooth teaches sending a message to the Bluetooth enabled mobile device, corresponding to supported data capability of the Bluetooth enabled data capture device. [Supra 12.3].

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

356. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.4]. In my opinion, Hiroishi-Kahn-Bluetooth teaches acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established. This limitation is broken down into constituent steps below:

[1.4.1] acquiring new data in the Bluetooth enabled data capture device,

357. As I explain in [Supra 12.4], Hiroishi-Kahn-Bluetooth teaches acquiring new data in the Bluetooth enabled data capture device.

[1.4.2] wherein new data is data acquired after the paired secure Bluetooth connection is established;

358. Hiroishi teaches that the mobile phone 40 and the digital camera 50 are connected by a Bluetooth connection. Hiroshi, [0066]-[0067] ("The photographing system 10 according to this embodiment is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth.")

359. Hiroshi teaches that the camera the digital camera 50 can be operated remotely by the mobile phone 40. TTI-1011, [0043], ("the photographing system 10 according to this embodiment is a system wherein various keys provided to the mobile phone 40 are used to remotely operate the digital camera 50 by transmitting various instruction information"), [0072], ("In Step 100 of the same drawing, a determination is made as to whether a remote operation mode is set up"). Hiroishi discloses that the digital camera 50 can be instructed to take a photograph through the remote (Bluetooth) connection. When the KB key is pressed on the mobile phone 40, it causes the digital camera 50 "to release the shutter" taking a picture and acquiring new data, [0096]. A POSITA would thus understand that because the instructions for remotely taking a picture are received over Bluetooth, the "new data is acquired after the paired secure Bluetooth connection is established".

[1.5] detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device,
wherein detecting and signaling the new data for transfer comprises:

360. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.5]. In my opinion, Hiroishi-Kahn-Bluetooth teaches detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer. [Supra 12.5].

[1.6] receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection;

361. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.6]. In my opinion, Hiroishi-Kahn-Bluetooth teaches receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection. [Supra 12.6].

[1.7] receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection;

362. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.7]. In my opinion, Hiroishi-Kahn-Bluetooth teaches receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection. [Supra 12.7].

[1.8] enabling event notification on Bluetooth enabled data capture device, corresponding to new data;

363. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.8]. In my opinion, Hiroishi-Kahn-Bluetooth teaches enabling event notification on

Bluetooth enabled data capture device, corresponding to new data. [Supra 12.6].

[1.9] determining existence of the new data for transfer; and

364. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.9]. In my opinion, Hiroishi-Kahn-Bluetooth teaches determining existence of the new data for transfer. [Supra 12.7].

[1.10] sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection,
wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth enabled data capture device;

365. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.10]. In my opinion, Hiroishi-Kahn-Bluetooth teaches sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth enabled data capture device. Supra [12.7].

[1.11] encrypting, using cryptographic encryption key, the new data acquired in the Bluetooth enabled data capture device; and

366. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.11]. In my opinion, Hiroishi-Kahn-Bluetooth teaches encrypting, using cryptographic encryption key, the new data acquired in the Bluetooth enabled data capture device. [Supra 12.9].

[1.12] transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure

Bluetooth connection,
wherein the Bluetooth enabled mobile device has access to the internet,
wherein the Bluetooth enabled mobile device is configured to receive the encrypted data and obtain the new data from the encrypted data using cryptographic encryption key,
wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data,
wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method,
wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server,
wherein the user identifier uniquely identifies a particular user of internet service provided by the remote internet server.

367. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.12]. In my opinion, Hiroishi-Kahn-Bluetooth teaches transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data and obtain the new data from the encrypted data using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service

provided by the remote internet server. Supra [12.10].

[6.P] A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:

368. To the extent the preamble is limiting, the Hiroishi-Kahn-Bluetooth combination renders obvious [6.P]. In my opinion, Hiroishi-Kahn-Bluetooth teaches a method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device. Supra [1.P].

[6.1] performing at a Bluetooth enabled data capture device:

369. The Hiroishi-Kahn-Bluetooth combination renders obvious [6.1]. In my opinion, Hiroishi-Kahn-Bluetooth teaches performing at a Bluetooth enabled data capture device. Supra [1.1].

[6.2] establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;

370. The Hiroishi-Kahn-Bluetooth combination renders obvious [6.2]. In my opinion, Hiroishi-Kahn-Bluetooth teaches 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. Supra [1.2].

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

371. The Hiroishi-Kahn-Bluetooth combination renders obvious [6.3]. In my opinion, Hiroishi-Kahn-Bluetooth teaches acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established. Supra [1.4].

[6.4] detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device,
wherein detecting and signaling the new data for transfer comprises:

372. The Hiroishi-Kahn-Bluetooth combination renders obvious [6.4]. In my opinion, Hiroishi-Kahn-Bluetooth teaches detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer. Supra [1.5].

[6.5] receiving a message from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, to register for data signal notifications,
wherein the data signal notifications correspond to existence of new data for transfer on the Bluetooth enabled data capture device;

373. The Hiroishi-Kahn-Bluetooth combination renders obvious [6.5]. In my opinion, Hiroishi-Kahn-Bluetooth teaches receiving a message from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, to register for data signal notifications, wherein the data signal notifications correspond to existence of new data for transfer on the Bluetooth enabled data capture device. Supra [12.6]. As discussed above (see supra [12.4]),

after the mobile phone sends a thumbnail transmission instruction to the camera, the mobile phone "waits" to receive the thumbnails from the camera. A POSITA would recognize the thumbnail transmission instruction to the camera as the mobile phone registering for the data signal notifications (the thumbnails).

[6.6] determining existence of the new data for transfer; and

374. The Hiroishi-Kahn-Bluetooth combination renders obvious [6.6]. In my opinion, Hiroishi-Kahn-Bluetooth teaches determining existence of the new data for transfer. Supra [1.9].

[6.7] creating a new data object on the Bluetooth enabled data capture device, wherein the new data object comprises new data, data associated with new data and a data signal notification,
wherein data signal notification is a time-stamp attribute inside the data object,
wherein the data signal notification corresponds to existence of new data for transfer, and
wherein the time-stamp corresponds to a time when new data was acquired;

375. The Hiroishi-Kahn-Bluetooth combination renders obvious [6.7]. In my opinion, Hiroishi-Kahn-Bluetooth teaches creating a new data object on the Bluetooth enabled data capture device, wherein the new data object comprises new data, data associated with new data and a data signal notification, wherein data signal notification is a time-stamp attribute inside the data object, wherein the data signal notification corresponds to existence of new data for transfer, and wherein the time-stamp corresponds to a time when new data was acquired. For example, Kahn teaches that "the image data already includes timestamp information (i.e.,

timestamp indicating when the image is captured)." TTI-1017, [0060]. *See also* Supra [15.9].

[6.8] encrypting, using cryptographic encryption key, the new data object in the Bluetooth enabled data capture device; and

376. The Hiroishi-Kahn-Bluetooth combination renders obvious [6.8]. In my opinion, Hiroishi-Kahn-Bluetooth teaches encrypting, using cryptographic encryption key, the new data object in the Bluetooth enabled data capture device. Supra [1.11].

[6.9] transferring the encrypted data object from the Bluetooth enabled data capture device to the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection,
wherein the Bluetooth enabled mobile device has access to the internet,
wherein the Bluetooth enabled mobile device is configured to receive the encrypted data object and obtain the new data and the data signal notification from the encrypted data object using cryptographic encryption key,
wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data,
wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method,
wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server,
wherein the user identifier uniquely identifies a particular user of internet service provided by a remote internet server.

377. The Hiroishi-Kahn-Bluetooth combination renders obvious [6.9]. In my opinion, Hiroishi-Kahn-Bluetooth teaches transferring the encrypted data object from the Bluetooth enabled data capture device to the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, wherein

the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data object and obtain the new data and the data signal notification from the encrypted data object using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by a remote internet server. Supra [1.12].

378. The "**the data signal notification**" is disclosed by Hiroishi as the thumbnails that are "transmitted according to the thumbnail transmission instruction information" to the mobile phone 40. Hiroishi, [0067], [0084]. The mobile phone sends the camera a thumbnail transmission instruction, which is a message to enable the "data signal notification" corresponding to the new data. The full-resolution images stored in memory are the "new data," and therefore, the thumbnails are the "data signal notification" of the capture of the new data. Likewise, the thumbnails "correspond" to the new data and serve as a data signal notification because the thumbnails are a lower resolution representation of the

full-resolution images stored in memory on the camera.

[2] The method of claim 1, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.

379. The Hiroishi-Kahn-Bluetooth combination renders obvious [2]. In my opinion, Hiroishi-Kahn-Bluetooth teaches Bluetooth capability is provided internally in the Bluetooth enabled data capture device. For example, Hiroishi teaches that the camera includes an internal short-range wireless communications module, TTI-1011, Fig. 4, [0058], ("The digital camera 50 is further provided with…a communication unit 59 for performing communication corresponding to the predetermined communication protocol with the mobile phone 40."), .TTI-1011, [0067], ("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.").

[7] The method of claim 6, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.

380. The Hiroishi-Kahn-Bluetooth combination renders obvious [7]. In my opinion, Hiroishi-Kahn-Bluetooth teaches Bluetooth capability is provided internally in the Bluetooth enabled data capture device. Supra [2].

[11] The method of claim 6, wherein the time-stamp is either absolute time or relative time.

381. The Hiroishi-Kahn-Bluetooth combination renders obvious [11]. In my opinion, Hiroishi-Kahn-Bluetooth teaches the time-stamp is either absolute

time or relative time. For example, Kahn teaches that it was well known at the time to include a time-stamp with image data. *See, e.g.*, Kahn, [0008] (describing prior art systems that recorded information about the data/time (time-stamp) that an image was captured). In Kahn, the time-stamp records absolute time for when the image was recorded.

[13] The method of claim 12, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

382. The Hiroishi-Kahn-Bluetooth combination renders obvious [13]. In my opinion, Hiroishi-Kahn-Bluetooth teaches the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data. For example, Hiroishi discloses the new data can be at least image data, TTI-1011, [0068], [0079], [0093] and video data but states that the embodiment is not limited to still pictures. Id., [0123].

[4] The method of claim 1, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

383. The Hiroishi-Kahn-Bluetooth combination renders obvious [4]. In my opinion, Hiroishi-Kahn-Bluetooth teaches the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data. Supra [13].

[9] The method of claim 6, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

384. The Hiroishi-Kahn-Bluetooth combination renders obvious [9]. In my opinion, Hiroishi-Kahn-Bluetooth teaches the new data for transfer comprises one

or more of audio data, video data, image data, text data, or digital data. Supra [13].

[14] The method of claim 12, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

385. The Hiroishi-Kahn-Bluetooth combination renders obvious [14]. In my opinion, Hiroishi-Kahn-Bluetooth teaches event notification corresponds to creation of new data for transfer or change in status of new data for transfer. For example, Hiroishi discloses that after a user selects a picture transfer from the event notification thumbnail images, the full resolution image is processed by the camera for transfer to the mobile phone. Hiroishi, [0084] ("Step 124, wherein a selected image transmission processing is performed, the selected image transmission processing is that the digital image data corresponding to the image selected by the operator of the mobile phone 40 from a plurality of images shown by the thumbnails").

[5] The method of claim 1, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

386. The Hiroishi-Kahn-Bluetooth combination renders obvious [5]. In my opinion, Hiroishi-Kahn-Bluetooth teaches event notification corresponds to creation of new data for transfer or change in status of new data for transfer. Supra [14].

[10] The method of claim 6, wherein said data signal notification corresponds to creation of new data for transfer or change in status of new data for transfer.

387. The Hiroishi-Kahn-Bluetooth combination renders obvious [10]. In

my opinion, Hiroishi-Kahn-Bluetooth teaches said data signal notification corresponds to creation of new data for transfer or change in status of new data for transfer. Supra [14].

[16] The method of claim 15, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

388. The Hiroishi-Kahn-Bluetooth combination renders obvious [16]. In my opinion, Hiroishi-Kahn-Bluetooth teaches the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data. Supra [13].

[17] The method of claim 15, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

389. The Hiroishi-Kahn-Bluetooth combination renders obvious [17]. In my opinion, Hiroishi-Kahn-Bluetooth teaches event notification corresponds to creation of new data for transfer or change in status of new data for transfer. Supra [14].

[18] The method of claim 6, wherein the time-stamp is either absolute time or relative time.

390. The Hiroishi-Kahn-Bluetooth combination renders obvious [18]. In my opinion, Hiroishi-Kahn-Bluetooth teaches the time-stamp is either absolute time or relative time. Supra [11].

C. Ground 2A—Claims 1–12, 4-7, 9-14 are obvious over Singh129 in view of Bluetooth

391. Singh129 provides the same disclosure as the ’030 patent. Although

this disclosure is insufficient to satisfy the written description requirement for the reasons explained above in Section VII, it would have been obvious in view of the Bluetooth Standard to modify Singh129's data acquisition device and/or mobile device to: (1) send a message to the Bluetooth enabled mobile device / receive a message from the Bluetooth enabled data capture device, corresponding to a supported data capability of the Bluetooth enabled data capture device and (2) encrypt/decrypt the new data.

392. A person of ordinary skill in the art would have been motivated to make these modifications to Singh129's data acquisition device and would have reasonably expected to succeed for the same reasons it would have been obvious to add these features to the Hiroishi/Takahashi and Hiroishi/Kahn combinations. Sections XI.A-B, *supra*.

[12.P]A method for transferring data to a remote internet server by a Bluetooth enabled mobile device comprising:

393. The Singh129-Bluetooth combination performs the method recited in element [12.P]. The Singh129-Bluetooth system performs a method for transferring data (e.g., data acquired by Singh129's digital data capture device 201) to a remote internet server (e.g., Singh129's publishing service 401 and/or website, such as "FlickrTM, PicasaTM, YouTubeTM, eBay®, etc.") by a Bluetooth enabled mobile device (Singh129's mobile device 202). Singh129, Abstract, [0042], Figs. 1-5 (and related descriptions).

[12.1] providing a software module on the Bluetooth enabled mobile device, wherein the software module on the Bluetooth enabled mobile device is configured to perform steps comprising:

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

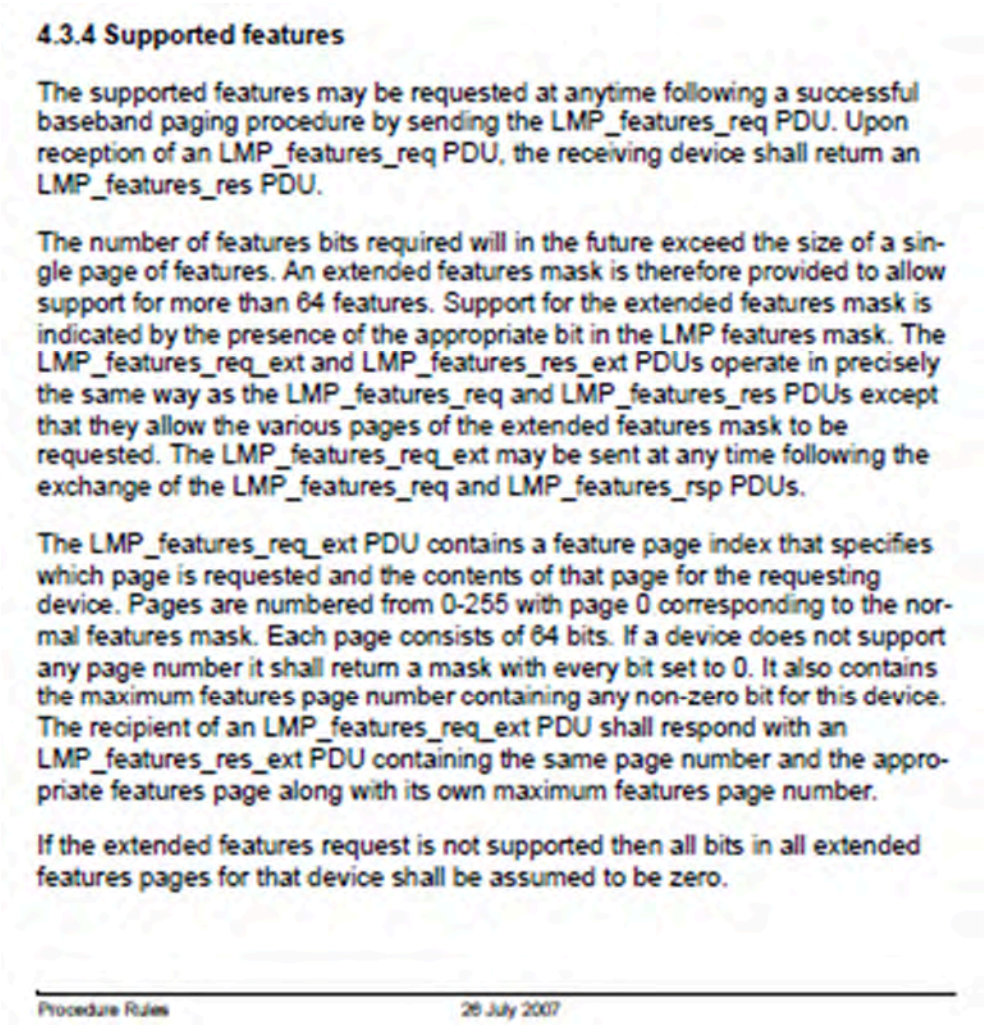
[12.2] establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein paired secure Bluetooth connection uses cryptographic encryption key;

395. The Singh129-Bluetooth combination performs step [12.2]. The Singh129-Bluetooth combination establishes a paired secure connection (a two-way Bluetooth connection) between the Bluetooth enabled mobile device (Singh129's mobile device 202) and a Bluetooth enabled data capture device (Singh129's digital data capture device 201), wherein the paired secure Bluetooth connection uses cryptographic encryption key(s). Singh129, [0021].

[12.3] receiving a message from the Bluetooth enabled data capture device, corresponding to supported data capability of the Bluetooth enabled data capture device;

396. The Singh129-Bluetooth combination performs step [12.3]. As previously explained, in the Singh129-Bluetooth combination, Singh129's digital data capture device 201 is modified to send a message corresponding to its supported data capability and the client application 203 on Singh129's Bluetooth enabled mobile device 202 is modified to receive that message. Indeed, the

Singh129-Bluetooth combination's connection complies with the Bluetooth protocols available in 2007, which described the option to exchange between the Bluetooth devices information regarding supported features. *See* Bluetooth Core Specification V2.1, Section 4.3.4 (shown below).



4.3.4 Supported features

The supported features may be requested at anytime following a successful baseband paging procedure by sending the LMP_features_req PDU. Upon reception of an LMP_features_req PDU, the receiving device shall return an LMP_features_res PDU.

The number of features bits required will in the future exceed the size of a single page of features. An extended features mask is therefore provided to allow support for more than 64 features. Support for the extended features mask is indicated by the presence of the appropriate bit in the LMP features mask. The LMP_features_req_ext and LMP_features_res_ext PDUs operate in precisely the same way as the LMP_features_req and LMP_features_res PDUs except that they allow the various pages of the extended features mask to be requested. The LMP_features_req_ext may be sent at any time following the exchange of the LMP_features_req and LMP_features_rsp PDUs.

The LMP_features_req_ext PDU contains a feature page index that specifies which page is requested and the contents of that page for the requesting device. Pages are numbered from 0-255 with page 0 corresponding to the normal features mask. Each page consists of 64 bits. If a device does not support any page number it shall return a mask with every bit set to 0. It also contains the maximum features page number containing any non-zero bit for this device. The recipient of an LMP_features_req_ext PDU shall respond with an LMP_features_res_ext PDU containing the same page number and the appropriate features page along with its own maximum features page number.

If the extended features request is not supported then all bits in all extended features pages for that device shall be assumed to be zero.

Procedure Rules 26 July 2007

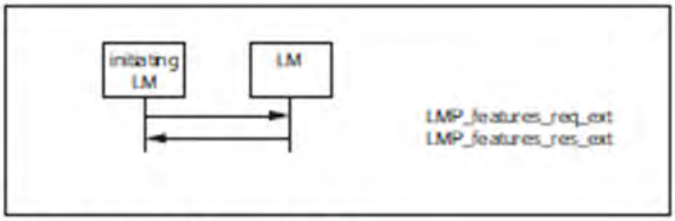
E.g., Bluetooth Core Specification V2.1, 441-442.

M/O	PDU	Contents
M	LMP_features_req	features
M	LMP_features_res	features
O(63)	LMP_features_req_ext	features page max supported page extended features
O(63)	LMP_features_res_ext	features page max supported page extended features

Table 4.22: PDUs used for features request.



Sequence 68: Request for supported features.



Sequence 69: Request for extended features.

397. As shown above, the max supported page is indicative of supported data capability of the Bluetooth enabled mobile device. Other examples of features that are reported include number of slots per packet (3 slot packets or 5 slot packets), Adaptive Frequency Hopping (AFH) capability, Channel Quality Driven Data Rate, and Enhanced Data Rate (EDR). Bluetooth Core Specification V2.1, 441-443 (explaining feature definitions).

[12.4] detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:

398. The Singh129-Bluetooth combination performs step [12.4]. The

Singh129-Bluetooth combination's client application 203 on the Bluetooth enabled mobile device detects new data (e.g., photographs) acquired by the Bluetooth enabled data capture device (Singh129's digital data capture device 201) for transfer to Singh129's mobile phone 202. Singh129, [0023]-[0027].

[12.5] sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;

399. The Singh129-Bluetooth combination performs step [12.5]. In the Singh129-Bluetooth combination, the detecting step (see Element [12.4]) includes sending a message (Singh129's polling message) to the Bluetooth enabled data capture device 201, over the established paired secure Bluetooth connection, to enable event notifications (the data capture device 201's response to the polling message or it signal to the client application 203 on creation of a new file) on the data capture device 201 corresponding to new data (e.g., photographs), wherein the new data is data acquired by data capture device after establishing the secure Bluetooth pairing connection between the data capture device and the mobile device. Singh129, Fig. 1, [0023]-[0027].

[12.6] enabling event notification listening on Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;

400. The Singh129-Bluetooth combination performs step [12.6]. In the Singh129-Bluetooth combination, the detecting step (*see* Element [12.4]) includes enabling event notification listening (using the file event listener in the client application 203) on the mobile device 202, to listen for event notifications ("signals") sent from the data capture device 201, over the established paired secure Bluetooth connection. Singh129, [0023]-[0027].

[12.7] receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and

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

[12.8] sending a request to the Bluetooth enabled data capture device, to get new data for transfer;

402. The Singh129-Bluetooth combination performs step [12.8]. In the Singh129-Bluetooth combination, the detecting step (*see* Element [12.4]) includes sending a request (a polling request) to the Bluetooth enabled data capture device 201, to get new data (e.g., a photograph) for transfer to the mobile device 202.

Singh129, [0023]-[0027].

[12.9] receiving, by the Bluetooth enabled mobile device, encrypted data corresponding to the new data over the established Bluetooth paired secure wireless connection and obtaining new data from the received encrypted data using cryptographic encryption key; and

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

[12.10] transferring the obtained new data along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.

404. The Singh129-Bluetooth combination performs step [12.10]. The

Singh129-Bluetooth combination's software module (client application) on the Bluetooth enabled mobile device 202 is configured to perform the step of transferring (via email) the obtained new data (e.g., a photograph) along with a user identifier (email address) to a remote internet server (publishing service 401), wherein the transferring step comprises configuring the obtained new data to comprise an action setting (user input) and a destination web address ("websites, for example, FlickrTM, PicasaTM, YouTubeTM, eBay®, etc.") of a remote internet server (the email server for the publishing server 401 and/or the servers for the selected websites), wherein the action setting comprises one of a remote procedure call (e.g., "XML-RPC") method and hypertext transfer protocol ("HTTP") method, and wherein the user identifier (email address) uniquely identifies a particular user (the user of Singh129's mobile device 202) of the internet service (publishing) provided by a remote internet server (publishing server 401 and/or the servers for the selected websites). Singh129, [0036], [0040], [0047].

[13] The method of claim 12, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

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

[14] The method of claim 12, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

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

[1.P] A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:

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

[1.1] performing at a Bluetooth enabled data capture device:

408. See Ground 2A, Element [12.2]-[12.7].

[1.2] establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;

409. See Ground 2A, Element [12.2].

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

410. See Ground 2A, Element [12.3].

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

411. See Ground 2A, Element [12.4]-[12.5].

[1.5] detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises:

412. See Ground 2A, Element [12.4]-[12.5].

[1.6] receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection;

413. See Ground 2A, Element [12.8].

[1.7] receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection;

414. See Ground 2A, Element [12.5].

[1.8] enabling event notification on Bluetooth enabled data capture device, corresponding to new data;

415. See Ground 2A, Element [12.5].

[1.9] determining existence of the new data for transfer; and

416. See Ground 2A, Element [12.4]-[12.8].

[1.10] sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection,
wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth enabled data capture device;

417. See Ground 2A, Element [12.7]

[1.11] encrypting, using cryptographic encryption key, the new data acquired in the Bluetooth enabled data capture device; and

418. See Ground 2A, Element [12.9].

[1.12] transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure

Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data and obtain the new data from the encrypted data using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by the remote internet server.

419. See Ground 2A, Element [12.9] (confirming that the Singh129-Bluetooth combination performs the step of transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection and that the Bluetooth enabled mobile device is configured to receive the encrypted data and obtain the new data from the encrypted data using cryptographic encryption key); Ground 2A, Element [12.10] (confirming that the mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by the remote internet server).

420. In the Singh129-Bluetooth combination, the mobile device 202 also

has access to the internet. Singh129, Figs. 4-5 (and related descriptions), [0039], [0042], [0044], [0047].

[2] The method of claim 1, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.

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

[4] The method of claim 1, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

422. See Ground 2A, Claim [13].

[5] The method of claim 1, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

423. See Ground 2A, Claim [14].

[6.P] A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:

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

[6.1] performing at a Bluetooth enabled data capture device:

425. See Ground 2A, Element [1.1].

[6.2] establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;

426. See Ground 2A, Element [1.2].

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

427. See Ground 2A, Element [1.4].

[6.4] detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises:

428. See Ground 2A, Element [1.5].

[6.5] receiving a message from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, to register for data signal notifications, wherein the data signal notifications correspond to existence of new data for transfer on the Bluetooth enabled data capture device;

429. See Ground 2A, Element [12.6].

[6.6] determining existence of the new data for transfer; and

430. See Ground 2A, Element [1.9].

[6.7] creating a new data object on the Bluetooth enabled data capture device, wherein the new data object comprises new data, data associated with new data and a data signal notification, wherein data signal notification is a time-stamp attribute inside the data object, wherein the data signal notification corresponds to existence of new data for transfer, and wherein the time-stamp corresponds to a time when new data was acquired;

431. See Ground 2B, Element [15.7]-[15.8].

[6.8] encrypting, using cryptographic encryption key, the new data object in the Bluetooth enabled data capture device; and

432. See Ground 2A, Element [1.11].

[6.9] transferring the encrypted data object from the Bluetooth enabled data capture device to the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device

is configured to receive the encrypted data object and obtain the new data and the data signal notification from the encrypted data object using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by a remote internet server.

433. See Ground 2A, Element [1.12].

[7] The method of claim 6, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.

434. See Ground 2A, Claim [2].

[9] The method of claim 6, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

435. See Ground 2A, Claim [13].

[10] The method of claim 6, wherein said data signal notification corresponds to creation of new data for transfer or change in status of new data for transfer.

436. See Ground 2A, Claim [14].

[11] The method of claim 6, wherein the time-stamp is either absolute time or relative time.

437. See Ground 2B, Claim [18].

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

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

the new data was acquired. A person of ordinary skill in the art would have been motivated to make this modification and would have reasonably expected to succeed for the same reasons it would have been obvious to add this feature to the Hiroishi/Takahashi and Hiroishi/Kahn combinations. See Sections XI.A-B, supra.

[15.P] A method for transferring data to a remoter internet server by a Bluetooth enabled mobile device comprising:

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

[15.1] performing at a Bluetooth enabled mobile device:

440. See Ground 2A, Element [12.1].

[15.2] establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein the secure paired Bluetooth connection uses cryptographic encryption key;

441. See Ground 2A, Element [12.2].

[15.3] detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:

442. See Ground 2A, Element [12.4].

[15.4] sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device

443. See Ground 2A, Element [12.5].

[15.5] enabling event notification listening on the Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;

444. See Ground 2A, Element [12.6].

[15.6] receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and

445. See Ground 2A, Element [12.7].

[15.7] sending a request to the Bluetooth enabled data capture device, to get new data object for transfer, wherein new data object comprises of new data, data associated with new data and time-stamp, and wherein the time-stamp corresponds to a time when new data was acquired;

446. The Singh129-Takahashi-Bluetooth combination performs step [15.7]. As explained in Ground 2A, Element [12.8], in the Singh129-Bluetooth combination, the step of detecting includes sending a request (a polling request) to the Bluetooth enabled data capture device, to get new data (e.g., a photograph) for transfer. In the Singh129-Bluetooth combination, the client application also sends a request to get a new data object comprising the new data (e.g., a photograph) and data associated with the new data ("associated files"). Singh129, [0023]-[0027]. In accordance with Takahashi, the new data object in the combination further includes a time-stamp that corresponds to a time when new data was acquired. TTI-1014 (Takahashi), [0070], ("The captured photograph is acquired…[a]t this time, a file name is generated using the user ID…and the time and date").

[15.8] receiving, by the Bluetooth enabled mobile device, encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection;

447. See Ground 2A, Element [12.9] (confirming that the client application

performs the step of receiving, by the mobile device 202, encrypted new data over the established Bluetooth paired wireless connection).

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

[15.9] obtaining new data, data associated with new data and time-stamp from the received encrypted data object using cryptographic encryption key; and

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

[15.10] sending the obtained new data and the obtained time-stamp along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service provided by a remote internet server.

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

[16] The method of claim 15, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.

451. See Ground 2A, Claim [13].

[17] The method of claim 15, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.

452. See Ground 2A, Claim [14].

[18] The method of claim 6, wherein the time-stamp is either absolute time or relative time.

453. The Singh129-Takahashi-Bluetooth combination performs the method of claim [18]. In the Singh129-Takahashi-Bluetooth combination, the time-stamp is either absolute time or relative time, in accordance with Takahashi. TTI-1014 (Takahashi), [0070] (teaching that the time is added based on an internal clock, which could indicate relative time or absolute time). Takahashi teaches that the time is added based on an internal clock, which could indicate relative time or absolute time. TTI-1014, [0070].

XI. INVALIDITY ANALYSIS OF THE '766 PATENT

A. Ground 1: Singh129 renders claims 1-15 obvious

454. Singh129 provides the same disclosure as the '766 patent. And Singh906 provides the same disclosure as the incorporated '802 application. Although this disclosure is insufficient to satisfy the written description requirement for the reasons explained above in Section VII, the disclosure nonetheless demonstrates that it would have been obvious in view of Singh906 to

modify Singh129's user preferences to include authentication credentials, to arrive at the Challenged Claims. 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."

455. A POSITA would have been motivated to make these modifications for several reasons. For example, a skilled artisan starting with Singh129 would naturally look to Singh906 because Singh129 incorporates by reference the '802 application that published as Singh906.

456. A POSITA would have been further motivated to make the proposed modifications because adding authentication credentials to Singh129's user preferences would have given the user more control over the publishing of their multimedia content.

457. Moreover, there was a known problem in the art of associating multimedia objects with user preferences, as shown in Singh129. However, Singh906's user preferences address that issue. And combining the teachings of

Singh129 and Singh906 was not beyond the level of ordinary skill. Indeed, Singh129 and Singh906 address the same problem of associating multimedia objects with user preferences. And Singh906's user preferences, which included authentication credentials, were a known way to address that problem.

458. A POSITA would have been further motivated to modify Singh129's client application to upload user authentication credentials to websites so that the client application can publish content on password protected websites without first sending those credentials to a publishing service. A person of ordinary skill in the art would have understood that this functionality would increase the speed at which content could be uploaded because it would reduce the number of data transmissions. For mobile devices with sufficient memory to store the content received from the data capture device, it also would have reduced the need to host a separate publishing service and therefore reduced complexity and cost. And even if the publishing service was retained, the mobile device would still be able to publish content to password protected sites when the publishing service was down (e.g., for maintenance or due to a power outage).

459. A POSITA would have been further motivated to modify Singh129 as described above because the publishing service may have its own website, as taught by Singh906. Thus, a person of ordinary skill would have been motivated to use that website to provide virtual spaces for its clients in addition to supporting

third-party websites, as taught by Singh129. TTI-1010, [0017], [0018], [0027].

460. Finally, a POSITA would have been motivated to use HTTP to upload the authentication credentials to websites because websites generally use HTTP for user authentication and Singh129's client application is already configured to communicate with the publishing service 401 using HTTP. TTI-1009, [0047].

461. A POSITA would have had a reasonable expectation of success when combining Singh129's disclosures as described above. Indeed, the proposed combination would have required no more than the application of known techniques (using authentication credentials and HTTP) to a known system (Singh129's system) in the same field of endeavor (media publishing) and from the same assignee (CellSpinSoft) to obtain the benefits described above. Furthermore, in the combination, each element performs the same predictable function as it does separately, without significantly hindering the functions performed by Singh129's system. Indeed, Singh129's system would have continued to perform all the functions it performed before the proposed modifications, including associating multimedia content with user preferences. Similarly, Singh906's user authentication functionality would continue to operate in the same way (*e.g.*, logging on to websites on the user's behalf), but the user information including authentication credentials would be provided by the mobile device rather than the publishing service.

462. The Singh129 combination renders obvious each element of the claims 1-15 of the ’766 patent.

[1.P]. A short-range wireless enabled data capture device, comprising:

463. To the extent the preamble is limiting, the Singh129/Singh906 combination renders obvious element [1.P]. For example, the Singh129/Singh906 combination includes digital data capture device 201 (*e.g.*, a camera), which includes Bluetooth communication device 201a that enables short-range wireless communication with Bluetooth enabled mobile device 202. TTI-1009, Figs. 2, 5.

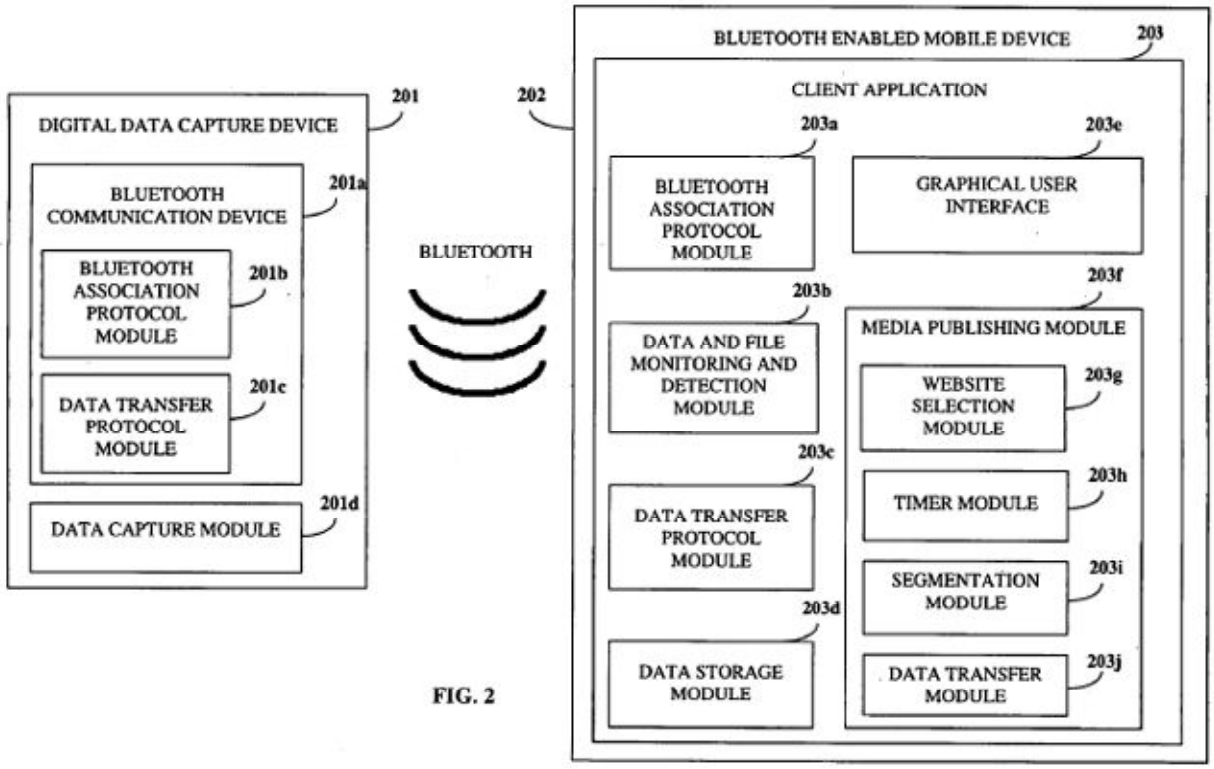


FIG. 2

TTI-1009, Fig. 2.

[1.1]. a memory device;

464. The Singh129/Singh906 combination renders obvious element [1.1].

The Singh129 combination's data capture device includes memory devices, e.g., "one or more microprocessors will receive instructions from a memory or like device", TTI-1009, [0048]. Memory card 302 is another example of a memory device that also has built in Bluetooth capability. TTI-1009, [0008], [0020], [0032], [0041], Figs. 2, 3A.

[1.2] a processor coupled to said memory device;

465. The Singh129/Singh906 combination renders obvious element [1.2]. The Singh129 combination's data capture device includes a processor (BT communication device 201a and/or the processor of data capture device 201) coupled to the memory device. TTI-1009, [0048] ("It will be readily apparent that the various methods and algorithms described herein may be implemented in a computer readable medium appropriately programmed for general purpose computers and computing devices. Typically, a processor, for e.g., one or more microprocessors will receive instructions from a memory or like device, and execute those instructions, thereby performing one or more processes defined by those instructions."').

[1.3] a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone,

466. The Singh129/Singh906 combination renders obvious element [1.3]. The Singh129 combination includes a short-range wireless communication device

(Bluetooth communication device 201a) configured to establish (via the Bluetooth protocol) a short-range paired wireless connection between the short-range wireless enabled data capture device 201 and a short-range wireless enabled cellular phone (Bluetooth enabled mobile device 202, which can be a cellular phone). TTI-1009, [0021]-[0022], [0046], Figs. 1-2.

[1.4] wherein establishing the short-range paired wireless connection comprises cryptographically authenticating identity of the short-range wireless enabled cellular phone, and

467. The Singh129/Singh906 combination renders obvious element [1.4]. In the Singh129 combination, establishing the short-range paired wireless connection comprises the data capture device cryptographically authenticating (via the Bluetooth protocol; specifically exchanging passkeys) the identity the cellular phone. TTI-1009, [0021]-[0022] ("A BT device that wants to communicate only with a trusted device can cryptographically authenticate the identity of another BT device.").

[1.5] wherein establishing the short-range paired wireless connection further comprises the short-range wireless enabled data capture device using an association protocol;

468. The Singh129/Singh906 combination renders obvious element [1.5]. In the Singh129 combination, establishing the short-range paired wireless connection comprises the data capture device using an association protocol (Bluetooth association protocol of BT association protocol module 201b). TTI-

1009, [0033] ("The BT communication device 201a comprises a BT association protocol module 201b…."), Fig. 2.

[1.6] data capture circuitry;

469. The Singh129/Singh906 combination renders obvious element [1.6]. The Singh129 combination includes a data capture circuity (data capture module 201d). TTI-1009, [0031], Fig. 2.

[1.7] said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry,

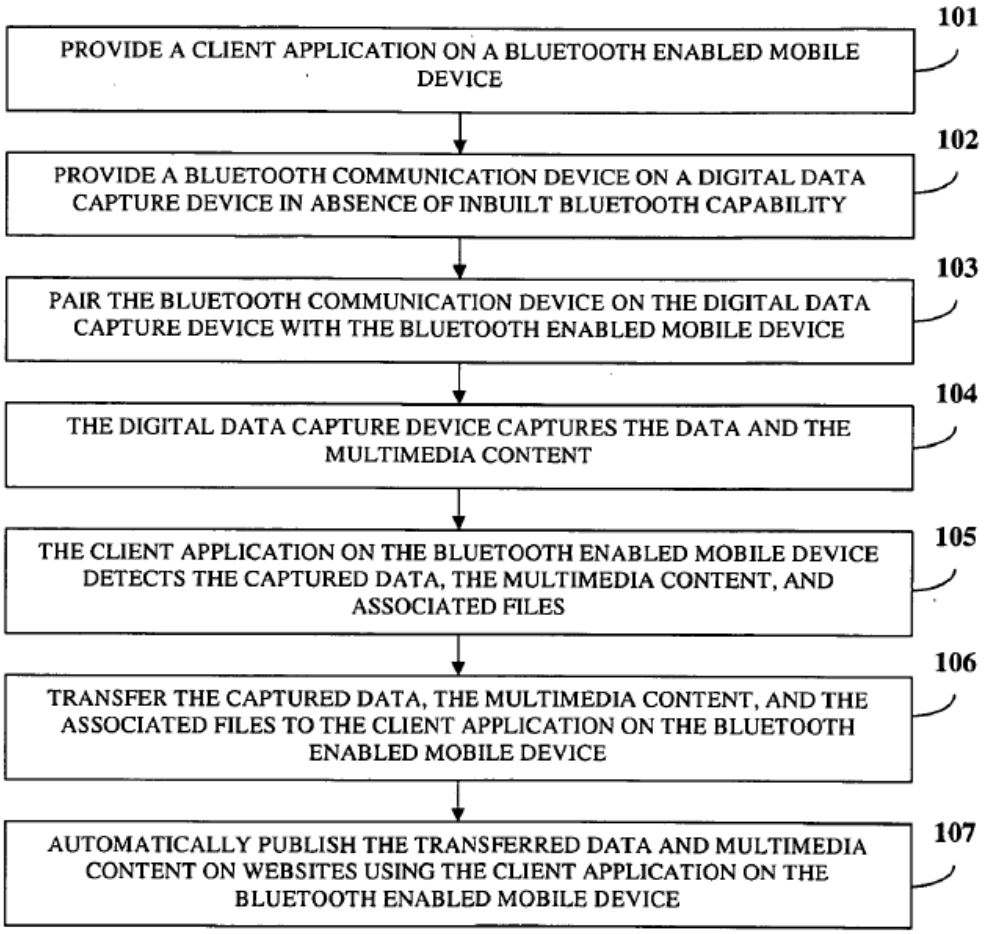
470. The Singh129/Singh906 combination renders obvious element [1.7]. The Singh129 combination's processor (*see* element [1.2]) is configured to acquire new-data (e.g., images) in the data capture device 201 using the data capture circuitry 201d. TTI-1009, [0033] ("The data capture module 201d captures the data and the multimedia content on the digital data capture device 201."), [0023], [0041], [0048], Figs. 1, 2, 5.

[1.8] wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;

471. The Singh129/Singh906 combination renders obvious element [1.8]. As shown in Figure 1 of Singh129, the new-data is data acquired (in step 104) after establishing the short-range wireless connection (in step 103) between the data capture device 201 and the cellular phone (mobile device 202). TTI-1009, Fig. 1, [0021]-[0023].

[1.9] said processor further configured to store the new-data in the memory device;

472. The Singh129/Singh906 combination renders obvious element [1.9]. The Singh129/Singh906 combination's processor (*see* element [1.2]) is further configured to store the new-data in the memory device (*see* element [1.1]). TTI-1009, [0023], [0041], Figs. 1, 5. As explained in Singh129, the "user captures 104 data and multimedia content using the digital data capture device 201." TTI-1009, [0023]; *see also* [0041] ("the user 502 may capture an image using the digital camera."). Accordingly, a POSITA would have understood that the processor stores the data and multimedia in the memory device.



TTI-1009, Fig. 1.

[1.10] said processor further configured to create a new-data object, wherein the new-data object comprises:

473. The Singh129/Singh906 combination renders obvious element [1.10]. In the Singh129/Singh906 combination, the processor is configured to create a new-data object (*e.g.*, the combination of "a signal to the client application 203 on creation of a new file," "captured data, [and/or] multimedia content, and the associated files"). TTI-1009, [0025]; *see also* TTI-1009, [0023]-[0028].

[1.11] 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;

474. *See* Ground 1, Element [1.10] ("the BT communication device 201a sends a signal to the client application 203 on creation of a new file").

[1.12] the acquired new-data; and

475. *See* Ground 1, Element [1.10] ("captured data, [and/or] multimedia content").

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

476. *See* Ground 1, Element [1.10] ("associated files").

[1.14] 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,

477. The Singh129/Singh906 combination renders obvious element [1.14]. As explained in Singh129, the processor is configured to transfer automatically the new-data object to the cellular phone over the established Bluetooth connection. TTI-1009, [0023] ("The digital data capture device 201 then automatically transfers 106 the captured data…."), [0025] ("In the push mode, the BT communication device 201a sends a signal to the client application 203 on creation of a new file. By implementation of a handshake protocol, the BT communication device 201a automatically transfers captured data, the multimedia content, and the associated files to the client application 203 on the mobile device 202.").

[1.15] 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,

478. The Singh129/Singh906 combination renders obvious element [1.15]. In the Singh129/Singh906 combination, the processor is configured to listen (using a file event listener in data and file monitoring and detection module 203b) to the signal to notify and receive (using BT association protocol module 201b and/or data transfer protocol module 201c) the new-data object over the established Bluetooth connection. TTI-1009, [0034], Figs. 1-2, [0025] ("A file event listener in the client application 203 listens for the signal from the digital data capture device 201. The user may then initiate the transfer by a press of a button or a key on the digital data capture device 201"), [0026], [0032]-[0033].

[1.16.1]-[1.16.2] wherein a mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the signal to notify and store the received new-data in a memory device of the cryptographically authenticated short-range wireless enabled cellular phone,

479. The Singh129/Singh906 combination renders obvious element [1.16.1]-[1.16.2]. In the Singh129/Singh906 combination a mobile client application (Singh129's client application 203 modified to include user authentication information as taught by Singh906) for the cellular phone is configured to process the signal to notify (using data and file monitoring and detection module 203b and/or Bluetooth association protocol module 203a) and

store the received new-data in a memory device (data storage module 203d) of the cellular phone. TTI-1009, [0033]-[0035] ("The data and file monitoring and detection module 203b of the client application 203 monitors and detects the capture of the data, the multimedia content, and the files associated with the captured data and the multimedia content. … The data storage module 203d stores the captured data, the multimedia content, and the associated files on the mobile device 202."), [0023]-[0025] (describing the push and pull modes), Fig. 2.

[1.17] 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

480. The Singh129/Singh906 combination renders obvious element [1.17]. In the Singh129/Singh906 combination, the single mobile client application (*see* element [1.9]) is configured to use HTTP to upload the received new-data and the user information to a user data publishing website ("for example, Flickr™, Picasa™, YouTube™, eBay®, etc.") over a cellular data network (Singh129's "cellular network"). TTI-1009, Figs. 1, 4, [0029], [0039], [0045] [0047]. As explained in Singh129, "client application 203 on the mobile device 202 … automatically publishes 107 the transferred data and multimedia content on one or more websites." TTI-1009, [0029], Fig. 1; *see also* [0045] (similar).

481. In the Singh129/Sing906 combination, Singh129's mobile client application is modified to upload user information including user credentials along

with the new-data to a publishing website based on the teachings of Singh906. TTI-1010, [0026] (discussing user authentication module 202e on the mobile device), [0028] (discussing transferring user preferences including authentication information to the publishing service 204), [0017] (discussing website of publishing service 204 and virtual spaces 205). In the combination, a person of ordinary skill would have been motivated based on the combined teachings to provide a system in which the client application sends new data with user information corresponding to authentication credentials to the publishing service website so that the new data may be published on virtual spaces on the publishing service website as well as on third-party websites. The credentials would be used to gain access to accounts on various websites. TTI-1010, [0027]-[0028], [0037]-[0038]. [0047]. Alternatively, a person of ordinary skill would have been motivated to provide for the mobile device to reach out to a private website requiring authentication directly and bypass the publishing service 401, in which case the credentials would be provided by the client application.

[1.18] 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.

482. The Singh129/Singh906 combination renders obvious element [1.18]. In the Singh129/Singh906 combination, the user information correspondence to a user identifier (*e.g.*, "a username and a password" in accordance with Singh906)

that uniquely identifies a particular user of the user data publishing website (*e.g.*, a user that "creates an account on a desired publication virtual space" in accordance with Singh906) and is used by the website (*e.g.*, to log on) to publish the new-data for private consumption. TTI-1010, [0038].

483. As explained in Singh906, if the website requires an account, the user "provides login information comprising a username and a password" to create an account." TTI-1010, [0038]. "The login information enables the publishing service 204 to access the multiple publication virtual spaces 205 configured by the user 201 on the mobile device." *Id*. "The publishing service 204 logs on to the publication virtual space of choice on the user's 201 behalf and publishes the user created multimedia content." *Id*. In the Singh129/Singh906 combination, the client application also logs on to the website on the user's behalf and publishes the content. *See* TTI-1009, [0044]-[0045], TTI-1010, [0017]-[0018].

2. The short-range wireless enabled data capture device of claim 1, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

484. The Singh129/Singh906 combination renders obvious claim 2. In the Singh129/Singh906 combination, the short-range paired wireless connection is a Bluetooth paired wireless connection. TTI-1009, Fig. 1, [0021].

3. The short-range wireless enabled data capture device of claim 1, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.

485. The Singh129/Singh906 combination renders obvious claim 3. In the Singh129/Singh906 combination, the new-data comprises "audio, video, text, and images." *Id*.; TTI-1009, [0011] ("The method and system disclosed herein thereby enables the user to capture data and multimedia content, for example, audio, video, text, and images, automatically upload the captured data and multimedia content onto a BT enabled mobile device, and publish the data and multimedia content on one or websites automatically or with minimal user intervention."), [0023] ("The data and multimedia content may, for example, comprise image files, audio files, video files, text files, or any combination thereof.").

[4.P] A system, comprising:

486. To the extent the preamble is limiting, the Singh129/Singh906 combination renders obvious element [4.P]. The Singh129/Singh906 combination includes a system comprising, among other things, a digital data capture device 201, a Bluetooth enabled mobile device 202, and a publishing service 401. TTI-1009, Figs. 1-5 and related descriptions.

[4.1]-[4.15]

487. *See* Ground 1, Elements [1.P]-[1.14]

[4.16]-[4.17] said cellular phone, comprising: a second memory device;

488. The Singh129/Singh906 combination renders obvious element [4.16]-[4.17]. The Singh129/Singh906 combination's cellular phone comprises a memory device (data storage module 203d). TTI-1009, Fig. 2, [0033], [0035] ("The data

storage module 203d stores the captured data, the multimedia content, and the associated files on the mobile device 202.").

[4.18] a second processor coupled to said second memory device;

489. The Singh129/Singh906 combination renders obvious element [4.18]. The Singh129/Singh906 combination's cellular phone comprises a processor coupled to the second memory device. TTI-1009, [0026] (disclosing a "mobile device 202 with limited memory and processing capabilities"), [0037] (similar), [0039] (similar), [0043] (similar), [0048] ("[T]he various methods and algorithms described [in Singh129] may be implemented in a computer readable medium appropriately programmed for general purpose computers and computing devices. Typically, a processor, for e.g., one or more microprocessors will receive instructions from a memory or like device, and execute those instructions, thereby performing one or more processes defined by those instructions.").

[4.19] a cellular network communication device configured to connect to the internet via the cellular data network;

490. The Singh129/Singh906 combination renders obvious element [4.19]. The Singh129/Singh906 combination's cellular phone comprises a cellular network communication (the portion of the phone that enables telephony data capabilities and/or data transfer module 203j) configured to connected to the internet via a cellular data network ("telephony network" or "cellular network"). TTI-1009, [0039] ("The network 402 may, for example, be a … cellular

network…."), [0047] ("the mobile phones may transfer data to the publishing service 401 over the telephony network at near broadband speeds … mobile phones equipped with both wireless network and telephony data capabilities may use either of the two to communicate with the publishing service 401").

[4.20] a second short-range wireless communication device configured to establish the short-range paired wireless connection between the cellular phone and the data capture device;

491. The Singh129/Singh906 combination renders obvious element 4.20. The Singh129/Singh906 combination's cellular phone comprises a second short-range wireless communication device (Bluetooth association protocol module 203a) configured to establish the short-range paired wireless (Bluetooth) connection between the cellular phone and the data capture device. TTI-1009, Fig. 2, [0033] ("The BT association protocol module 201b of the digital data capture device 201 and the BT association protocol module 203a of the client application 203 enable the pairing between the BT communication device 201a and the mobile device 202.")

[4.21]-[4.26]

492. *See* Ground 1, Elements [1.15]-[1.18].

5. The system of claim 4, wherein establishing the short-range paired wireless connection comprises the data capture device using an association protocol.

493. The Singh129/Singh906 combination renders obvious claim 5. In the Singh129/Singh906 combination, the establishing the short-range paired wireless

connection comprises the data capture device using an association protocol (the Bluetooth association protocol used by BT association protocol modules 201b and 203a). TTI-1009, Fig. 2, [0033].

Claims 6-7

494. *See* Ground 1, Claims 2-3.

8. The system of claim 4, wherein a graphical user interface (GUI) is provided in the cryptographically authenticated cellular phone, and wherein the graphical user interface (GUI) is for the received new-data.

495. The Singh129/Singh906 combination renders obvious claim 8. In the Singh129 combination, the cellular phone provides a GUI ("graphical user interface") for the received new-data. TTI-1009, Fig. 2, [0033] ("graphical user interface (GUI) 203e"), [0035] ("The user may also set timer and action settings for publishing the data and the multimedia content using the GUI 203 e."), and ("Claim 11 (similar).

[9.P] A short-range wireless enabled cellular phone, comprising:

496. To the extent the preamble is limiting, the Singh129/Singh906 combination renders obvious element [9.P]. *See* Ground 1, Element [4.4], [4.16].

[9.1]-[9.6]

497. *See* Ground 1, Elements [4.17]-[4.20],[4.4]-[4.6]. See Ground 1 [1.4].

[9.7]

498. *See* Ground 1, Element [4.21].

[9.8]-[9.9]

499. *See* Ground 1, Element [4.23], [4.8], [4.11]. See Ground 1, [1.10].

[9.10]-[9.12]

500. *See* Ground 1, Elements [4.12], [4.4], [4.8].

[9.13]

501. *See* Ground 1, Element [4.14].

[9.14]

502. *See* Ground 1, Elements [4.19], [1.16.1].

[9.15]

503. *See* Ground 1, Element [4.24].

[9.16]-[9.17]

504. *See* Ground 1, Elements [4.25]-[4.26].

Claims 10-12

505. *See* Ground 1, Claims 6, 7, 8.

[13.P]

506. *See* Ground 1, Element [4.P].

[13.1]-[13.13]

507. *See* Ground 1, Elements [4.1]-[4.14].

[13.14]-[13.15] said first processor further configured to receive a data transfer request from the short-range wireless enabled cellular phone, over the established short-range paired wireless connection, wherein the data transfer request is for the acquired new-data that was acquired by the short-range wireless enabled data capture device before receiving the data transfer request; and

508. The Singh129/Singh906 combination renders obvious element

[13.14]-[13.15]. In the Singh129/Singh906 combination, the processor of the data capture device is configured to receive a data transfer request (e.g., a poll for new data) from the cellular phone over the established Bluetooth connection. TTI-1009, [0023] ("In the pull mode, the client application 203 periodically polls the digital data capture device 201 to determine the creation of a new file in the digital data capture device 201. 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."), [0025], [0031]-[0035], Fig. 2.

[13.16] said first processor configured to transfer the new-data object to the short-range wireless enabled cellular phone over the established short-range paired wireless connection;

509. *See* Ground 1, Element [4.15].

[13.17]

510. *See* Ground 1, Element [4.21].

[13.18]-[13.19] receive a request through a graphical user interface (GUI) of the cryptographically authenticated short-range wireless enabled cellular phone for new-data and send a data transfer request to the short-range wireless enabled data capture device, over the established short-range paired wireless connection, wherein the data transfer request is for the acquired new-data that was acquired by the short-range wireless enabled data capture device before receiving the data transfer request;

511. The Singh129/Singh906 combination renders obvious element [13.18]-[13.19]. Singh129's mobile client application controls the processor to receive a request through a GUI of the cellular phone for new data, TTI-1009,

"[0035] ("The user may also set timer and action settings for publishing the data and the multimedia content using the GUI 203e."). Singh129's mobile client application also controls the processor to send a data transfer request (e.g., a poll for new data) to the data capture device over the established Bluetooth connection. TTI-1009, [0023] ("In the pull mode, the client application 203 periodically polls the digital data capture device 201 to determine the creation of a new file in the digital data capture device 201.").

512. *See* Ground 1, Element [13.14]-[13.15]. As explained in Singh129 (at [0023]), "the client application 203 periodically polls the digital data capture device 201 to determine the creation of a new file in the digital data capture device 201." Because the polling step is used to determine whether a new file is created, the poll (i.e., request) is a request for data that was acquired before receiving the request.

[13.20]-[13.23]

513. *See* Ground 1, Elements [4.20]-[4.22], [4.12].

Claims 14-15

514. *See* Ground 1, Claims 2-3.

B. Ground 2A: Kahn in view of Bluetooth renders claims 1-15 obvious

1. Kahn

515. U.S. Patent Publication 2004/0004737 to Kahn at al. ("Kahn"), titled,

"Imaging System Providing Automated Fulfillment of Image Photofinishing Based on Location," was filed on July 2, 2002 and published on January 8, 2004.

516. Kahn teaches an imaging system that includes a camera, which may be a wireless camera, coupled to a cellular phone by a connection that may be wireless. *See, e.g.*, Kahn, [0055], FIG. 3. Kahn teaches that the "camera device 310 is preferably a wireless camera device, such as camera device 100 (shown in FIG. 1A)." *Id*. The cellular phone can be a "host device" for the camera. *Id*. The cellular phone includes a global positioning module 325. The cellular phone determines a location ID, which is GPS derived longitude and latitude, and sends the location ID with the images to the image server. *See, e.g.*, *id*., [0058]. The server can use "the location information may be used to offer location-dependent promotions to the user." *See, e.g.*, *id*., [0051]. Kahn teaches that the "image data already includes timestamp information (i.e., timestamp indicating when the image is captured)". *See, e.g.*, *id*., [0060].

517. Kahn teaches a "system 300 includes a camera device 310, a host device 320, and a GPS (Global Positioning System) module 325." Kahn, [0055]. Further, "the host device 320 communicates with an online Web-based image management server 330… accessible via the Internet." Kahn, [0056].

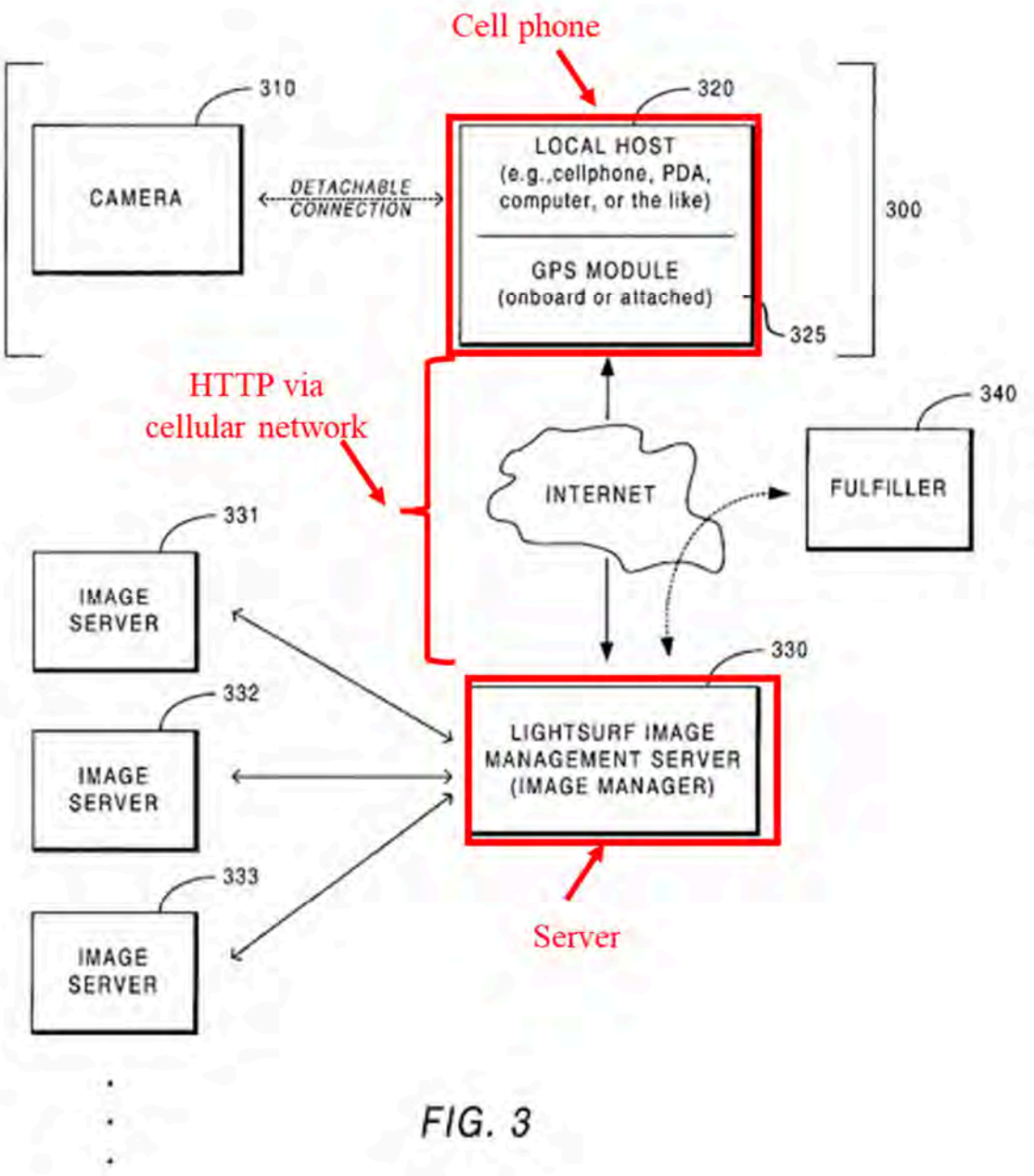


FIG. 3

Kahn, FIG. 3 (annotated).

518. In addition, Kahn teaches that the host device (i.e., the cellular phone) "communicates with an online Web-based image management server 330" using, for example, "HTTP protocol." Kahn, [0056].

519. Furthermore, in FIG. 4, Kahn "illustrates implementation of underlying functionality (i.e., processes) in the various modules of FIG. 3." Kahn, [0062]. The "system 400 includes the following functional modules: upload program 410, location API 420, camera memory/API 430, server-side image manager application 440, image servers 450, and database (e.g., Oracle) 460 for storing metadata information." Kahn, [0062].

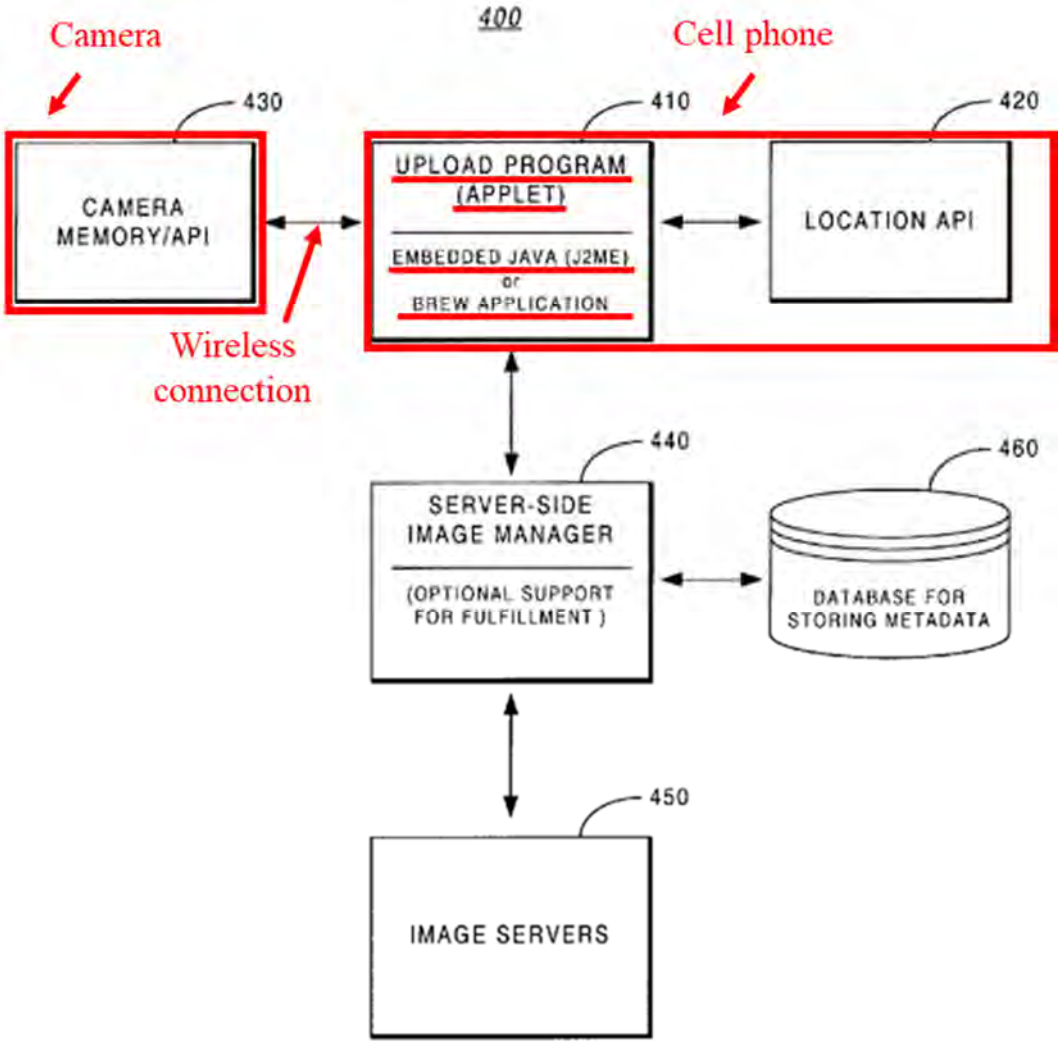


FIG. 4

Kahn, FIG. 4 (annotated).

2. Motivation to Combine Kahn with Bluetooth

Predictable combination of Kahn with Bluetooth

520. In the proposed combination, Kahn provides a system for image capture and transmission, wherein a digital camera uploads photos and related data

to a host device, such as a cell phone, for subsequent publishing via an image management server. The upload may be either automatic or in response to a transfer request. TTI-1017, [0062]. Kahn discloses a "detachable connection" and "cableless direct connection" and accordingly a POSITA would have understood that the connection between a camera and a cell phone would be a short-range wireless connection. At the very least, a POSITA would have been motivated to make that connection a short-range wireless connection, and specifically a Bluetooth connection, given the ubiquity and popularity of Bluetooth by the alleged Critical Date. TTI-1017, FIG. 3, [0045]. Bluetooth was undoubtedly the obvious choice. TTI-1011, (0066) (using Bluetooth for camera-phone connection). In the combination, Bluetooth provides the benefit of wireless connectivity using a well-known and powerful technology to connect Kahn's camera to Kahn's mobile phone.

521. The Bluetooth 2.1 Core Specification offers encryption as an option and a POSITA would use Bluetooth's encryption capability in the combination to secure the data transfer between the camera and the phone.

Motivation to Combine Kahn with Bluetooth

522. A POSITA would have been motivated to use Bluetooth to wirelessly connect the camera with the mobile phone in Kahn. First, Bluetooth was a well-known technique at the time of Kahn for connecting a mobile phone with a camera.

See, e.g., Hiroishi, [0066]-[0067]. A POSITA reviewing Kahn would have known to use such as well-know and ubiquitous short-range wireless communication technology to connect the camera with the mobile phone.

523. In addition, Kahn describes using a stand-alone GPS module to provide GPS information to the camera or mobile phone. *See, e.g.*, Kahn, [0055]. A POSITA would have recognized that a mobile phone, like that in Kahn would have included Bluetooth functionality. A POSITA would have recognized that by the alleged critical date, mobile phones typically had Bluetooth technology installed. For example, all iPhone models had Bluetooth. See, e.g., https://support.apple.com/en-us/112445 (archived Apple support page stating that the original iPhone used Bluetooth 2.0+EDR). A POSITA would have been motivated to use that Bluetooth functionality to also form a wireless connection between the camera and the phone, and would have selected the most current Bluetooth version available, which by July, 2007 was Bluetooth 2.1.

524. A POSITA would have had a reasonable expectation of success implementing Bluetooth. First, Bluetooth was a well-known technology at the time, and a POSITA would have had the requisite skills to implement it. Second, the Bluetooth specification provides ample details to perform all of the Bluetooth operations necessary to establish a connection between two devices, pair the two devices, and communicate data between the two devices.

3. Analysis

Claim 1

[1.P] A short-range wireless enabled data capture device, comprising:

525. To the extent the preamble is limiting, The Kahn-Bluetooth combination renders obvious [1.P]. Kahn-Bluetooth teaches or suggests a short-range wireless enabled data capture device. For example, Kahn discloses "an imaging device capable of capturing a plurality of images." Kahn, Abstract, [0018]. Kahn teaches "[a] camera device 310 is a stand-alone unit that is occasionally (or persistently) connected to the host device 320, which may be any device capable of hosting the camera device 310. For example, host device 320 may comprise a cellular phone, a PDA (personal data assistant) with wireless connectivity, or the like." Kahn, [0055].

526. In FIG. 3, Kahn illustrates a "system 300 [that] includes a camera device 310, a host device 320, and a GPS (Global Positioning System) module 325. The camera device 310 is preferably a wireless camera device, such as camera device 100 (shown in FIG. 1A), that either includes wireless connectivity itself or connects to a local host with wireless connectivity." Kahn, [0055].

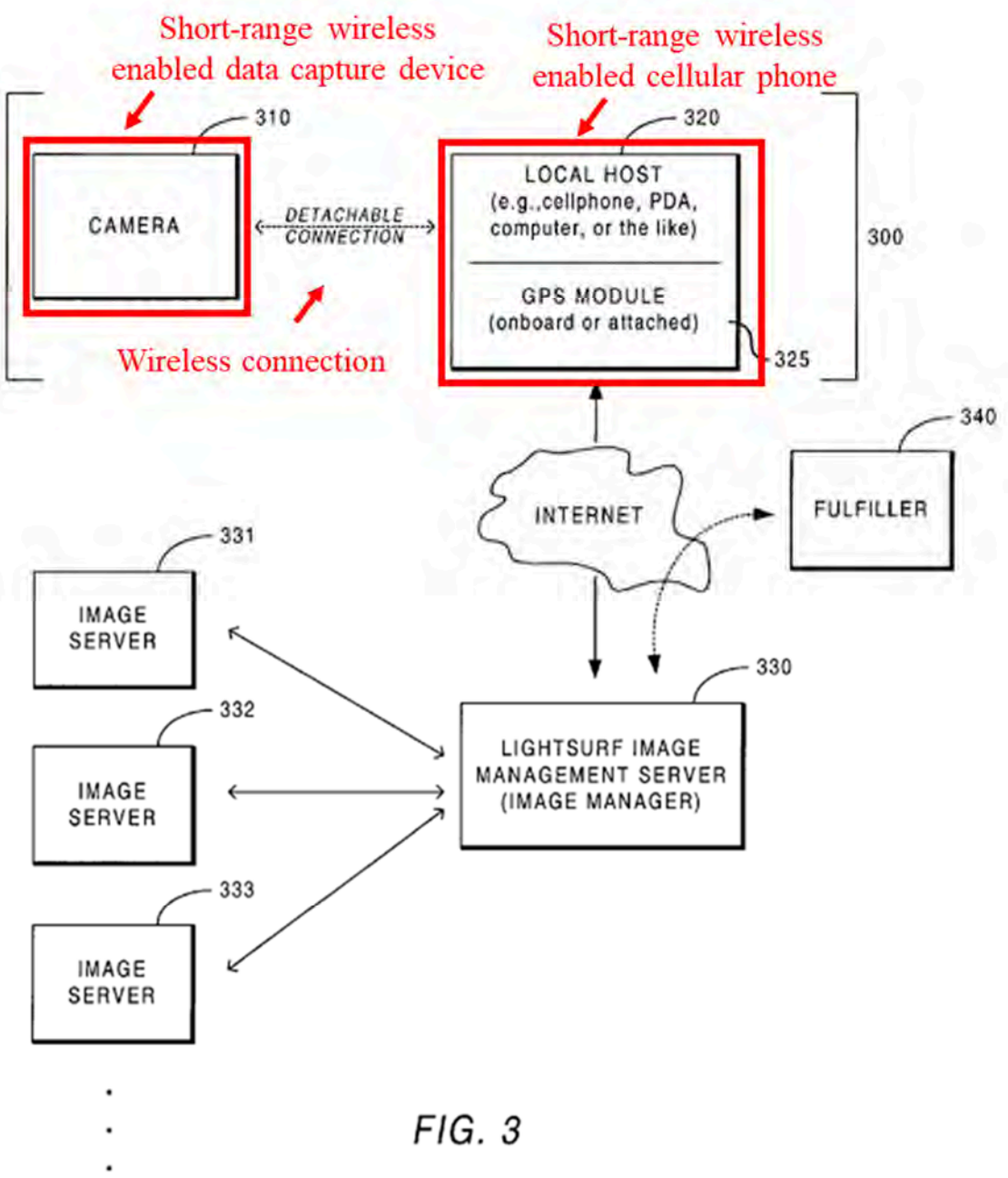


FIG. 3

527. Kahn, FIG. 3 (annotated). Kahn, [0023] ("FIG. 3 is a high-level block diagram illustrating the basic components that comprise the environment in which the present embodiment may be implemented.")

528. Kahn refers to a "detachable connection" and "cableless direct

connection." Id., FIG. 3, [0045]. In the combination, a POSITA would use Bluetooth for the connection from camera to phone, particularly given that Bluetooth was the short-range wireless technology of choice by 2007. Thus, as discussed in the motivation to combine section, a POSITA would have been motivated, and found it obvious, to use Bluetooth for the "detachable connection" between camera and phone. TTI-1017, FIG. 3, [0045].

[1.1] a memory device;

529. The Kahn-Bluetooth combination renders obvious [1.1]. Kahn-Bluetooth teaches or suggests a memory device. For example, Kahn teaches "captured image data is transferred over the system bus 130 to the computer 140 which performs various image processing functions on the image data before storing it in its internal memory." Kahn, [0035].

530. Kahn discloses a "system 300 [that] includes a camera device 310, a host device 320, and a GPS (Global Positioning System) module 325. The camera device 310 is preferably a wireless camera device, such as camera device 100 (shown in FIG. 1A), that either includes wireless connectivity itself or connects to a local host with wireless connectivity." Kahn, [0055], FIGs. 1A, 3.

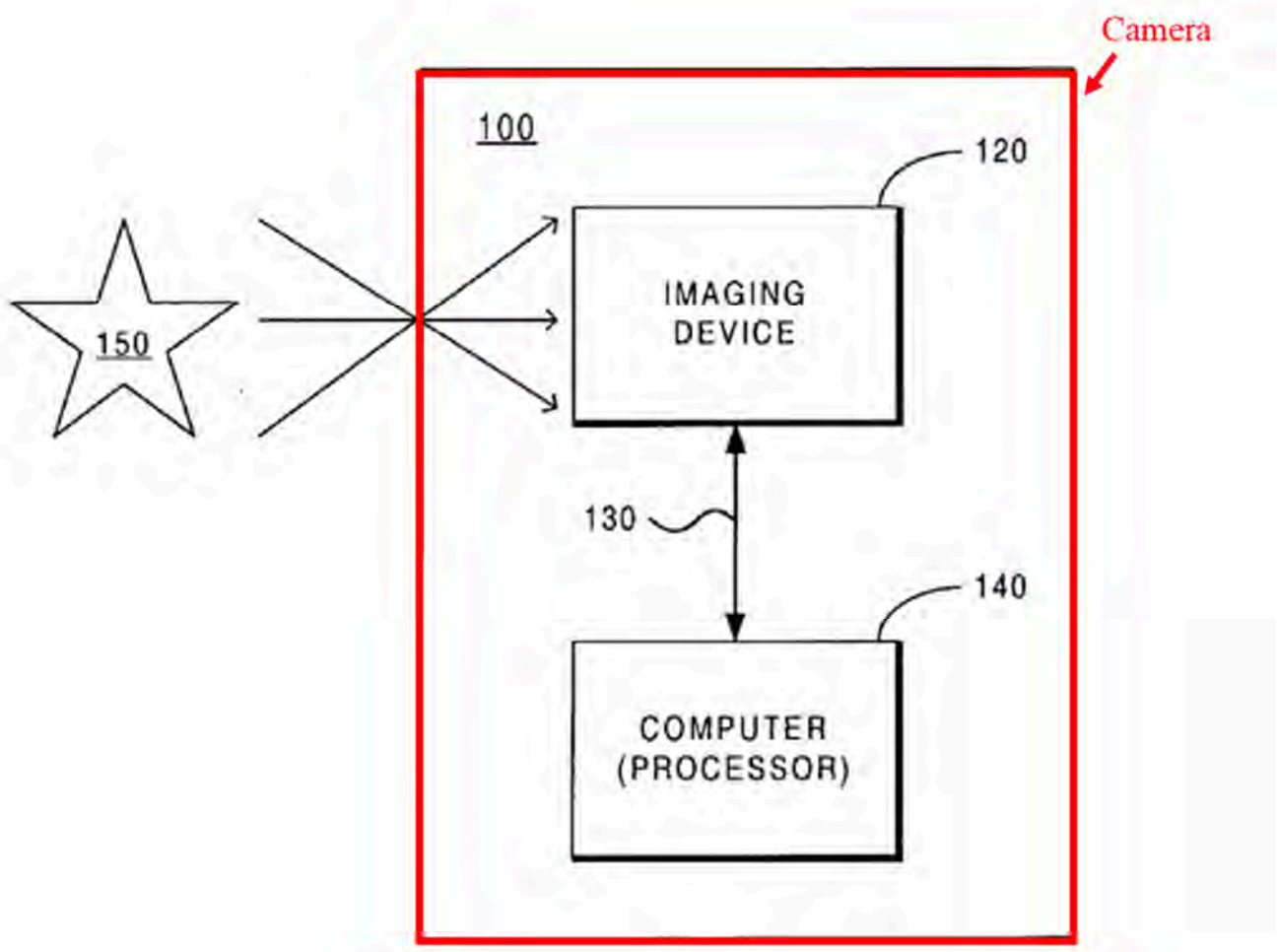


FIG. 1
(PRIOR ART)

Kahn, FIG. 1 (annotated). Kahn, [0020] ("FIG. 1 is a very general block diagram of a digital camera suitable for implementing the present invention.")

531. As below above in FIG. 2B, Kahn illustrates "[a] conventional onboard processor or computer 140 is provided for directing the operation of the digital camera 100 and processing image data captured on the imaging device 120.

FIG. 2B is a block diagram of the processor or computer 140. As shown, the system bus 130 provides connection paths between the imaging device 120, an (optional) power management 262, a processor (CPU) 264, a random-access memory (RAM) 266, an input/output (I/O) controller 280, a non-volatile memory 282, a removable memory interface 283, and a liquid crystal display (LCD) controller 290. Removable memory 284 connects to the system bus 130 via the removable memory interface 283. Alternately, the camera 100 (and therefore the onboard computer 140) may be implemented without the removable memory 284 or the removable memory interface 283." Kahn, [0042].

532. Further, Kahn discloses that "[t]e digital camera 100 includes several memory components. The memory (RAM) 266 is a contiguous block of dynamic memory that may be selectively allocated to various storage functions. Dynamic random-access memory is available from a variety of vendors, including, for instance, Toshiba of Japan, Micron Technology of Boise, Id., Hitachi of Japan, and Samsung Electronics of South Korea. The non-volatile memory 282, which may typically comprise a conventional read-only memory or flash memory, stores a set of computer-readable program instructions to control the operation of the camera 100. The removable memory 284 serves as an additional image data storage area and may include a non-volatile device, readily removable and replaceable by a camera 100 user via the removable memory interface 283. Thus, a user who

possesses several removable memories 284 may replace a full removable memory 284 with an empty removable memory 284 to effectively expand the picture-taking capacity of the camera 100. The removable memory 284 is typically implemented using a flash disk. Available vendors for flash memory include, for example, SanDisk Corporation of Sunnyvale, Calif. and Sony of Japan. Those skilled in the art will appreciate that the digital camera 100 may incorporate other memory configurations and designs that readily accommodate the image capture and processing methodology of the present invention." Kahn, [0044].

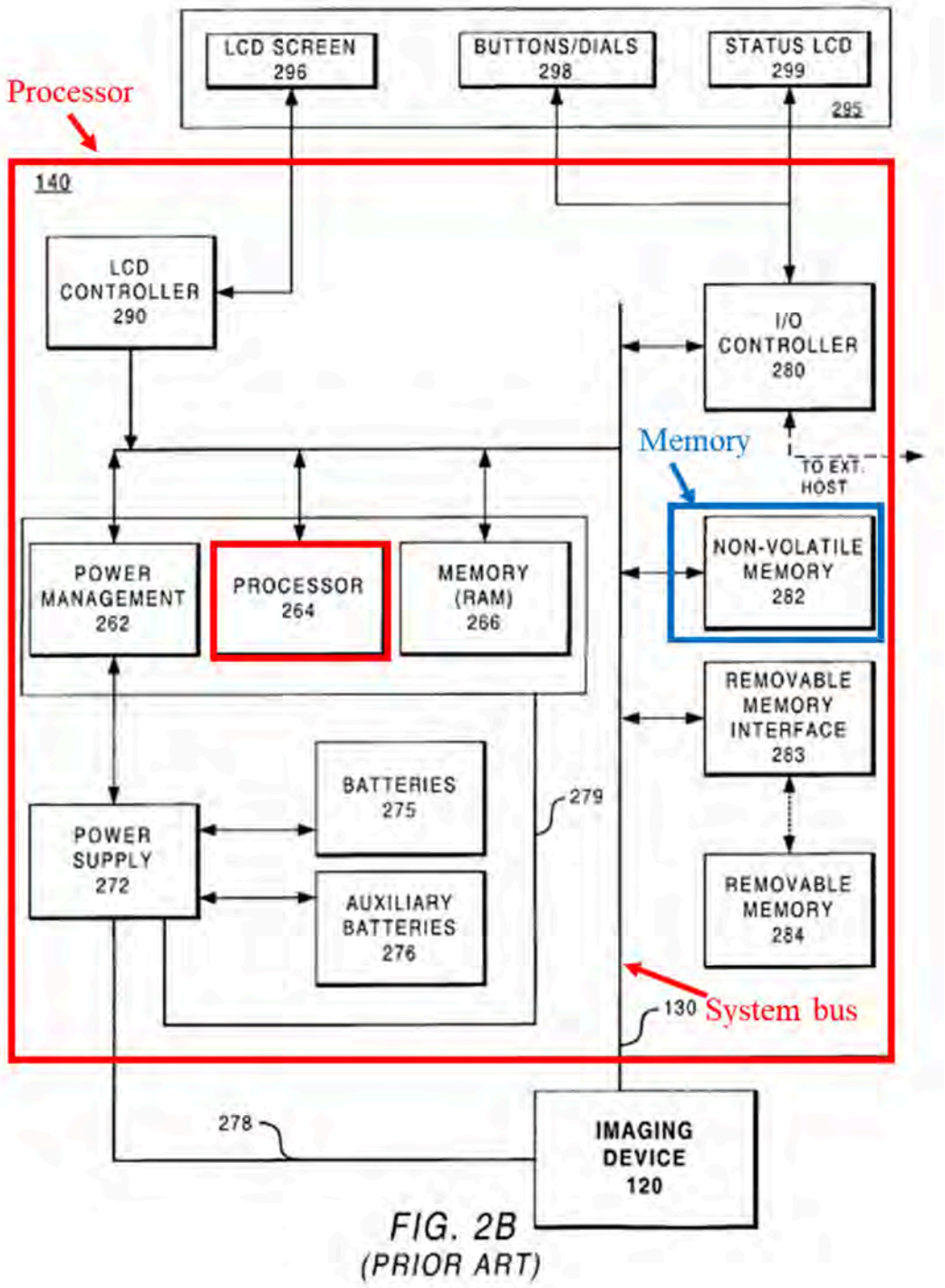


FIG. 2B
(PRIOR ART)

Kahn, FIG. 2B (annotated). Kahn, [0022] ("FIG. 2B is a block diagram of the processor or computer used for the digital imaging device of FIG. 2A.")

[1.2] a processor coupled to said memory device;

533. The Kahn-Bluetooth combination renders obvious [1.2]. Kahn-Bluetooth teaches or suggests a processor coupled to said memory device. For example, Kahn discloses "the digital camera 100 comprises an imaging device 120, a system bus 130, and a processor or computer 140 (e.g., microprocessor-based unit)." Kahn, [0033]. See also, id., [0034]-[0035], [0045].

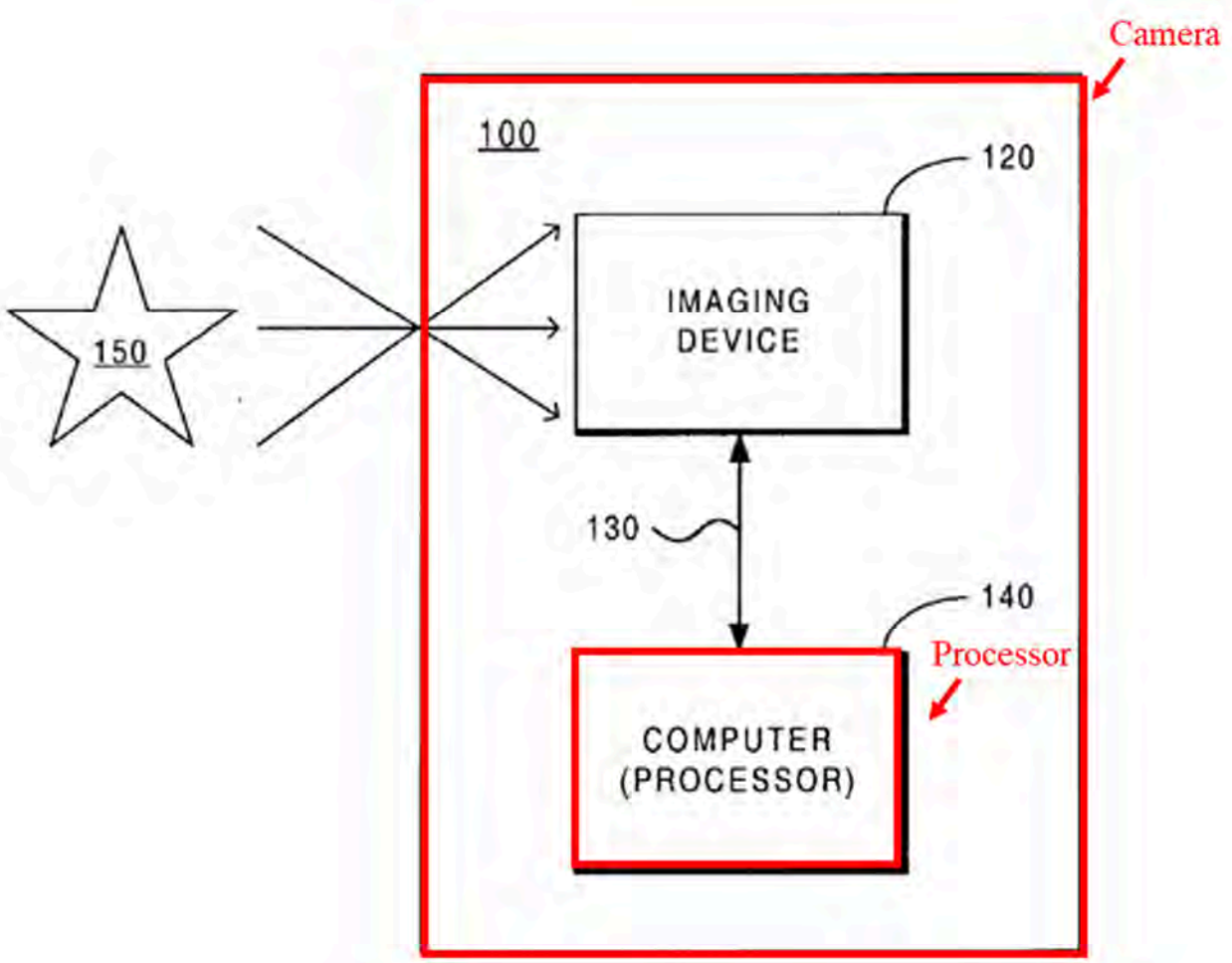


FIG. 1
(PRIOR ART)

Kahn, FIG. 1 (annotated). Kahn, [0020] ("FIG. 1 is a very general block diagram of a digital camera suitable for implementing the present invention.")

534. FIG 2B. in Kahn shows processor 264 coupled to memories via bus 130 including memory (RAM) 266, non-volatile memory 262, and removable memory 284 (via interface 283). Kahn, [0042) ("[a] conventional onboard

processor or computer 140 is provided for directing the operation of the digital camera 100 and processing image data captured on the imaging device 120. FIG. 2B is a block diagram of the processor or computer 140 …the system bus 130 provides connection paths between the imaging device 120, an (optional) power management 262, a processor (CPU) 264, a random-access memory (RAM) 266, an input/output (I/O) controller 280, a non-volatile memory 282, a removable memory interface 283, and a liquid crystal display (LCD) controller 290.").

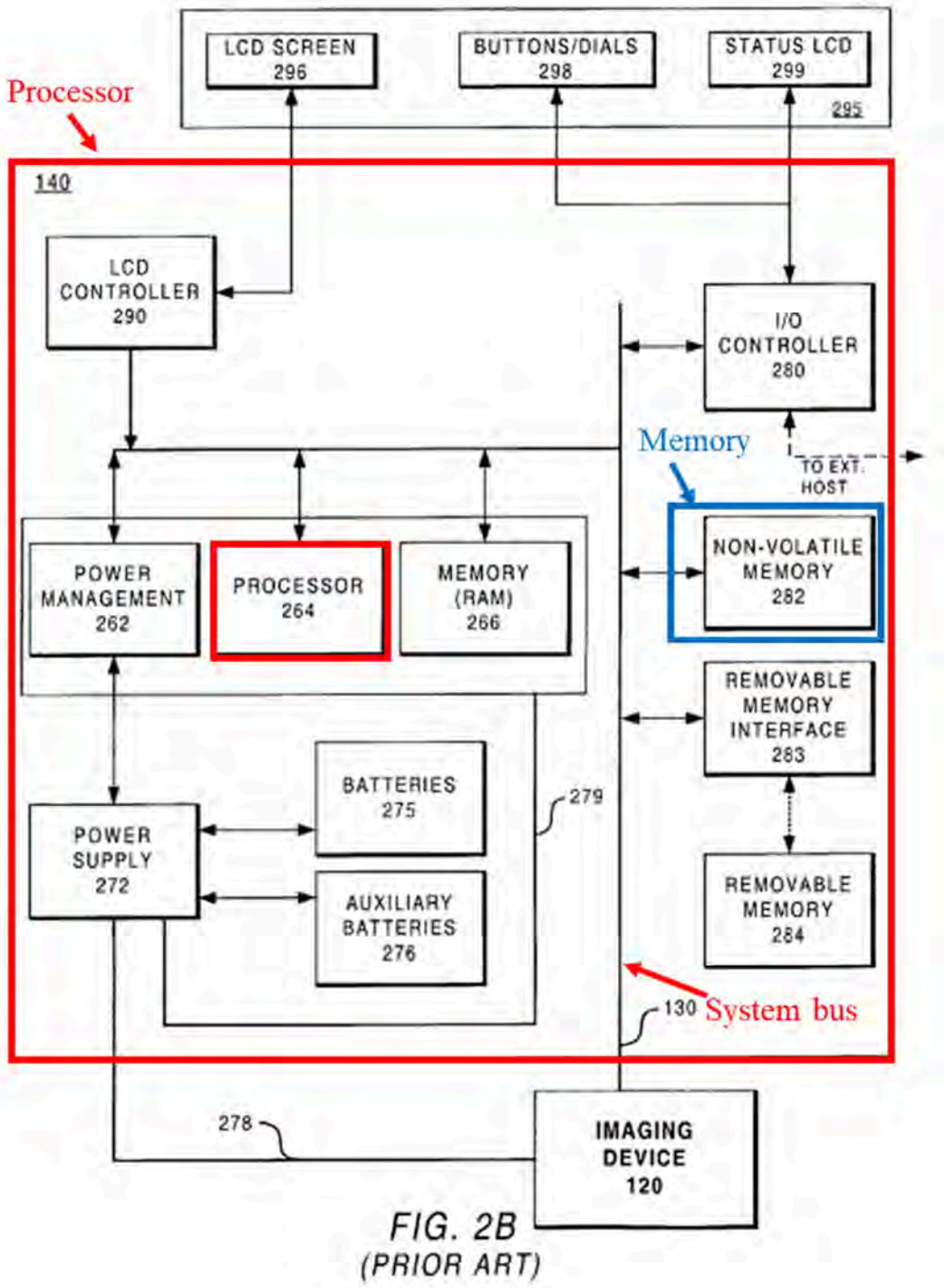


FIG. 2B
(PRIOR ART)

Kahn, FIG. 2B (annotated). Kahn, [0022] ("FIG. 2B is a block diagram of the processor or computer used for the digital imaging device of FIG. 2A.")

535. Further, Kahn discloses, "[t]he processor (CPU) 264 typically

includes a conventional processor device (e.g., microprocessor) for controlling the operation of camera 100. Implementation of the processor 264 may be accomplished in a variety of different ways. For instance, the processor 264 may be implemented as a microprocessor (e.g., MPC823 microprocessor, available from Motorola of Schaumburg, Ill.) with DSP (digital signal processing) logic blocks, memory control logic blocks, video control logic blocks, and interface logic. Alternatively, the processor 264 may be implemented as a "camera on a chip (set)" using, for instance, a Raptor II chipset (available from Conextant Systems, Inc. of Newport Beach, Calif.), a Sound Vision Clarity 2, 3, or 4 chipset (available from Sound Vision, Inc. of Wayland, Mass.), or similar chipset that integrates a processing core with image processing periphery. Processor 264 is typically capable of concurrently running multiple software routines to control the various processes of camera 100 within a multithreaded environment." Kahn, [0043].

[1.3] a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone;

536. The Kahn-Bluetooth combination renders obvious [1.3]. Kahn-Bluetooth teaches or suggests a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone. For example, Kahn discloses "[t]he digital camera 100 also

typically includes several interfaces for communication with a camera user or with other systems and devices. For example, the I/O controller 280 is an interface device allowing communications to and from the computer 140. The I/O controller 280 permits an external host, such as a cell phone, personal digital assistant (PDA), computer, or the like (not shown), to connect to and communicate with the computer 140." Kahn, [0045]. "[A] digital camera that includes occasional [wireless] connectivity to a local host device (e.g., GPS-enabled cell phone, personal digital assistant (PDA), laptop computer, or the like).". Kahn, [0030].

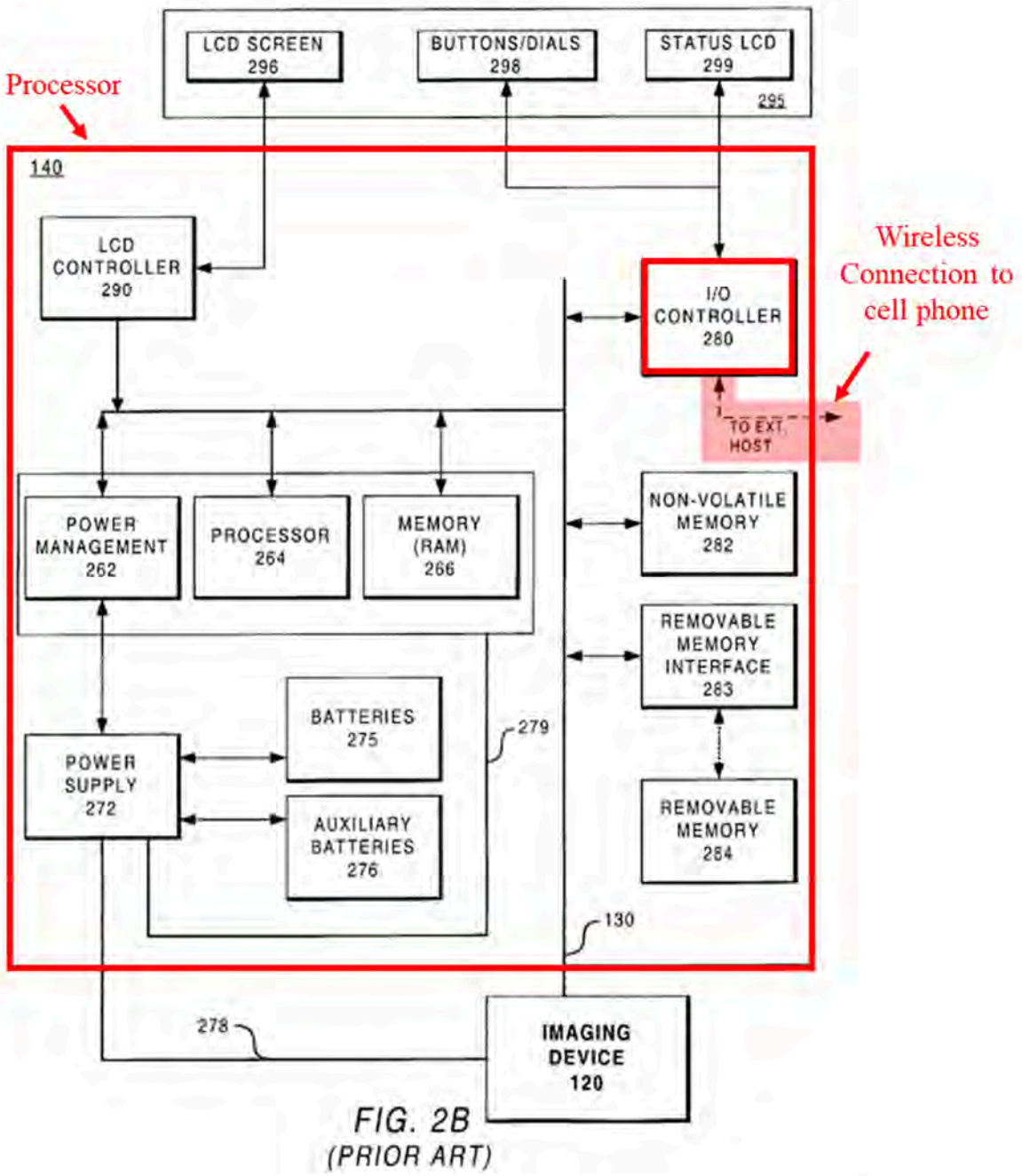


FIG. 2B
(PRIOR ART)

Kahn, FIG. 2B (annotated). Kahn, [0022] ("FIG. 2B is a block diagram of the processor or computer used for the digital imaging device of FIG. 2A.").

537. In FIG. 3, Kahn illustrates a "system 300 [that] includes a camera device 310, a host device 320, and a GPS (Global Positioning System) module

325. The camera device 310 is preferably a wireless camera device, such as camera device 100 (shown in FIG. 1A), that either includes wireless connectivity itself or connects to a local host with wireless connectivity. 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, which may be any device capable of hosting the camera device 310. For example, host device 320 may comprise a cellular phone, a PDA (personal data assistant) with wireless connectivity, or the like." Kahn, [0055].

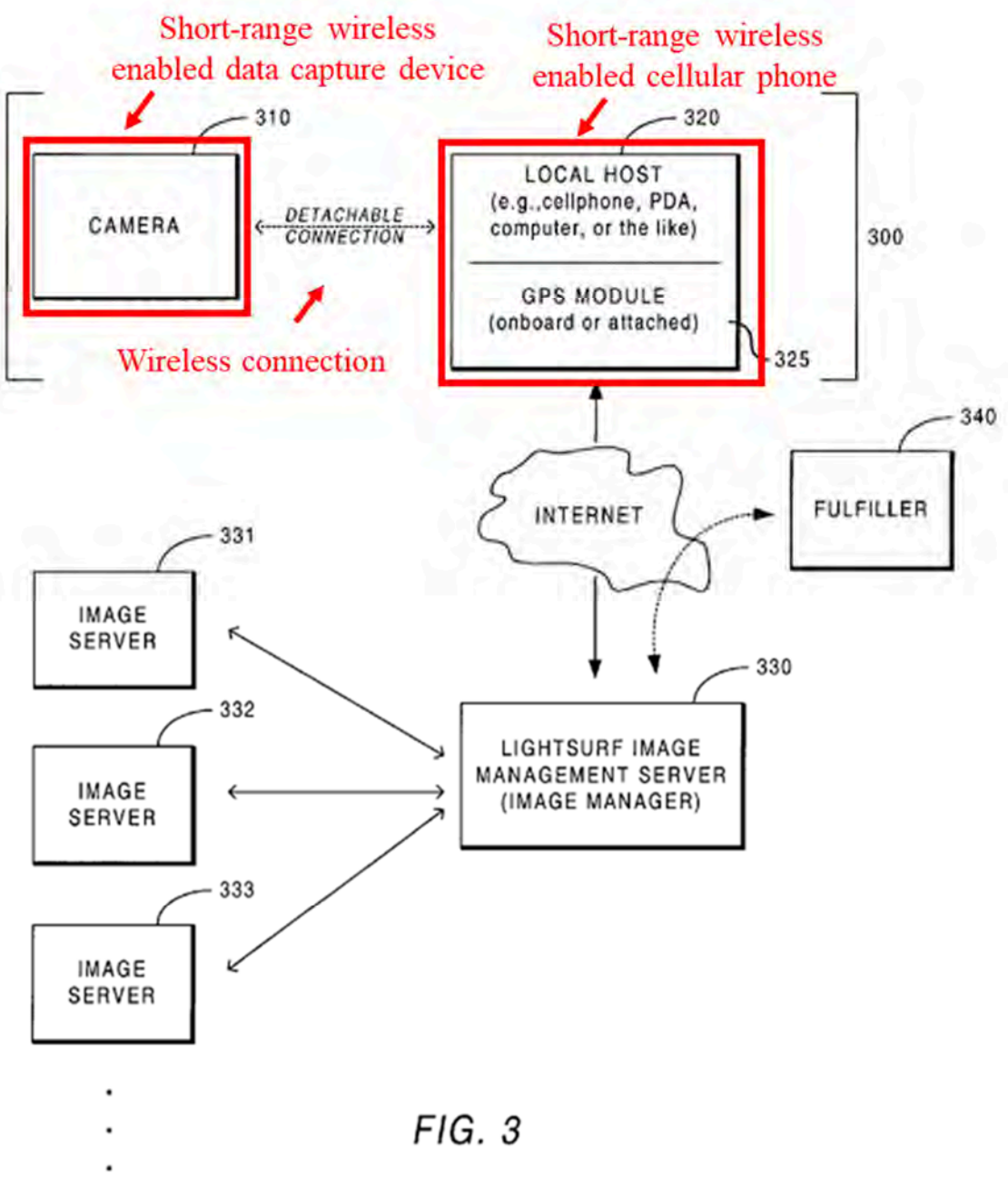


FIG. 3

Kahn, FIG. 3 (annotated). Kahn, [0023] ("FIG. 3 is a high-level block diagram illustrating the basic components that comprise the environment in which the present embodiment may be implemented.")

538. "The camera device 310 is preferably a wireless camera device, such

as camera device 100 (shown in FIG. 1A), that either includes wireless connectivity itself or connects to a local host with wireless connectivity." TTI-1017, [0055]. In the combination, the local wireless connectivity would use Bluetooth. See Ground 2A, [1.P]. Moreover, a POSITA would have been motivated to replace the cabled version of Khan with Bluetooth to gain the benefits of Bluetooth technology, which avoids both the cable and the wear and tear on the cable connector ports. Thus, in the combination the camera-phone connection in Kahn whether wired or wireless is replaced by a Bluetooth connection, as was typical in the art.

[1.4] wherein establishing the short-range paired wireless connection comprises cryptographically authenticating identity of the short-range wireless enabled cellular phone, and

539. The Kahn-Bluetooth combination renders obvious [1.4]. Kahn-Bluetooth teaches or suggests establishing the short-range paired wireless connection comprises cryptographically authenticating identity of the short-range wireless enabled cellular phone. As mentioned above (See Ground 2A, [1.3]) Kahn teaches a "detachable connection" and in some instances, "cableless direct connection." Kahn, FIG. 3, [0045]. While Kahn does not expressly specify the type of communication for the wireless detachable connection between the camera and the cell phone, a POSITA would find it as an obvious choice to utilize Bluetooth, which was a commonly used technique to establish a "detachable

connection", "cableless direct connection." Kahn, FIG. 3, [0045]. Bluetooth was a well-known wireless communication technique before the alleged Critical Date. Bluetooth could establish short-range paired wireless communication between a camera and a cell phone. Considering the benefits associated with Bluetooth and the similarities between Kahn and Hiroishi, a POSITA would be inclined to implement the teachings described by Hiroishi, which involves two-way wireless communication between a mobile phone and a digital camera via Bluetooth. Hiroishi states, "[t]he photographing system 10 according to this embodiment is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth. Bluetooth is a wireless transfer standard that uses a 2.4 GHz bandwidth and does not require any license to use, and can perform transfer of data signals in the range within about 10 m." Hiroishi, [0066].

540. In the combination, the short-range wireless connection is via Bluetooth and Bluetooth provides for the cryptographic authentication of the devices being paired. Bluetooth further provides the option of encryption to provide secure communications to prevent hacking or eavesdropping. TTI-1019, 412-425 (discussing pairing using a link key and discussing encryption of transmitted data), 1031-1038 (generating link keys and encryption keys); *See also* Kahn, [0045], [0096]. A POSITA would have used the cryptographic

authentication and would further have used Bluetooth encryption features when pairing the camera to the host mobile phone. For example, as discussed in the Bluetooth Core Specification V2.1, pairing between Bluetooth devices includes the generation and exchange of initialization keys created from a PIN, a random number, and a Bluetooth Device Address (BD_ADDR):

541. Referring to Bluetooth Core Specification 2.1 (July 2007), the pairing processes uses the BD_ADDR to form the initialization key (Kinit):

4.2.2 Pairing

When two devices do not have a common link key an initialization key (K_{init}) shall be created using either the pairing or Secure Simple Pairing procedures. When pairing is used, K_{init} shall be created based on a PIN, and a random number and a BD_ADDR. K_{init} shall be created as specified in [Part H] Section 6.3 on page 885. When both devices have calculated K_{init} the link key shall be created, and a mutual authentication is performed. The pairing procedure starts with a device sending an LMP_in_rand PDU; this device is referred to as the "initiating LM" or "initiator" in Section 4.2.2.1 on page 242 - Section 4.2.2.5 on page 245. The other device is referred to as the "responding LM" or "responder". The PDUs used in the pairing procedure are:

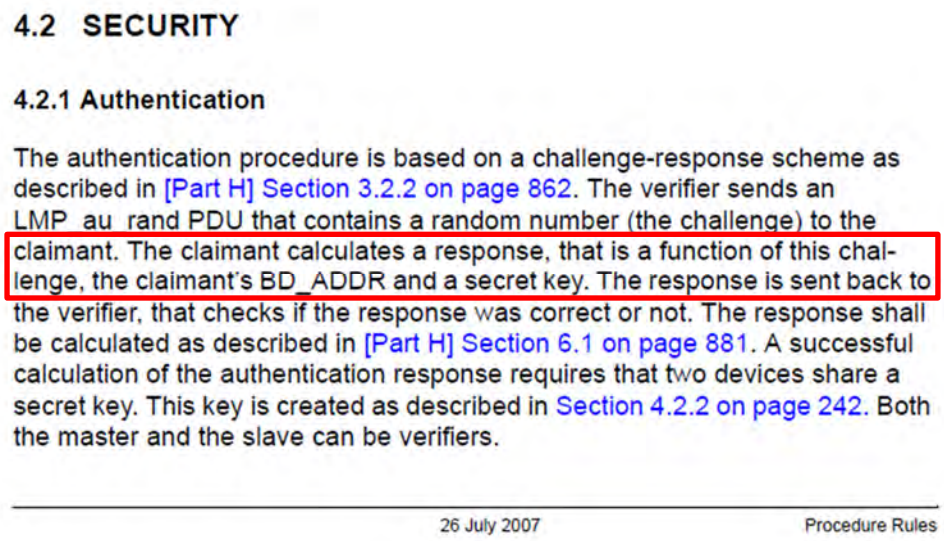
M/O	PDU	Contents
M	LMP_in_rand	random number
M	LMP_au_rand	random number
M	LMP_sres	authentication response
M	LMP_comb_key	random number
M	LMP_unit_key	key

Table 4.14: Pairing PDUs

All sequences described in Section 4 on page 223, including the mutual authentication after the link key has been created, shall form a single transaction. The transaction ID from the first LMP_in_rand shall be used for all subsequent sequences.

See, e.g., Bluetooth Core Specification, 412.

542. In another example, the Bluetooth Core specification describes the process for establishing a secure pairing as well as the obvious reasons behind secure pairing:



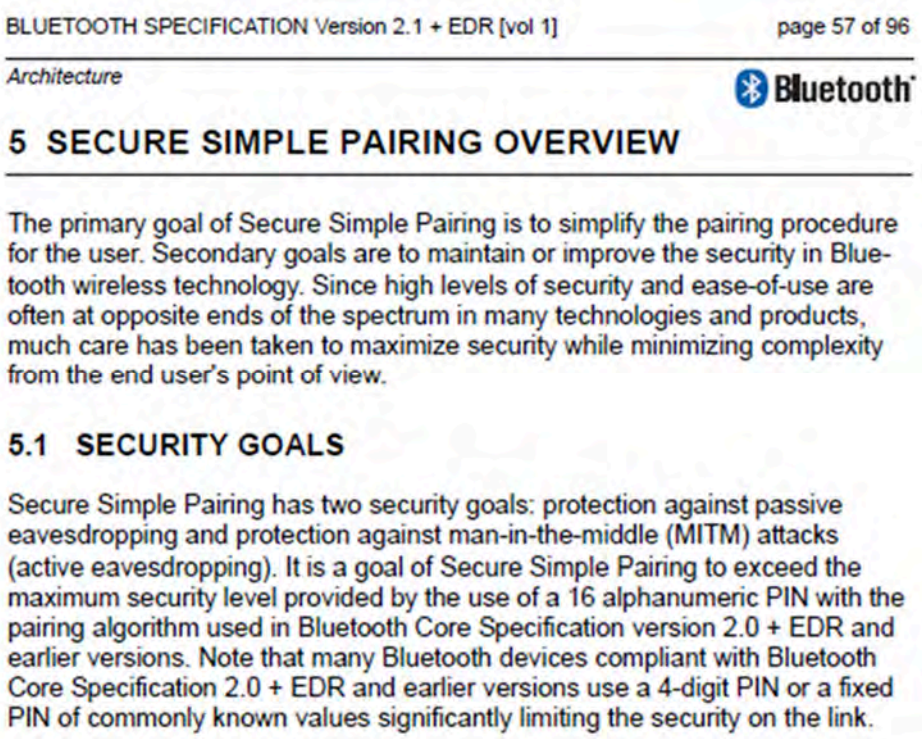
4.2 SECURITY

4.2.1 Authentication

The authentication procedure is based on a challenge-response scheme as described in [Part H] Section 3.2.2 on page 862. The verifier sends an LMP_au_rand PDU that contains a random number (the challenge) to the claimant. The claimant calculates a response, that is a function of this challenge, the claimant's BD_ADDR and a secret key. The response is sent back to the verifier, that checks if the response was correct or not. The response shall be calculated as described in [Part H] Section 6.1 on page 881. A successful calculation of the authentication response requires that two devices share a secret key. This key is created as described in Section 4.2.2 on page 242. Both the master and the slave can be verifiers.

See, e.g., Bluetooth Core Specification, 410. The Bluetooth core specification describes using BD_ADDR which represents Bluetooth device address. The BD_ADDR is a unique identifier that cryptographic authentication authenticates the identity of the connected device (for example authenticating between camera and cell phone while Bluetooth connection is being established.)

543. In another example, the Bluetooth Core specification describes a second process for establishing a secure pairing as well as the obvious reasons behind secure pairing ("protection against passive eavesdropping and protection against man-in-the-middle (MITM) attacks"):



BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 1] page 57 of 96

Architecture

Bluetooth

5 SECURE SIMPLE PAIRING OVERVIEW

The primary goal of Secure Simple Pairing is to simplify the pairing procedure for the user. Secondary goals are to maintain or improve the security in Bluetooth wireless technology. Since high levels of security and ease-of-use are often at opposite ends of the spectrum in many technologies and products, much care has been taken to maximize security while minimizing complexity from the end user's point of view.

5.1 SECURITY GOALS

Secure Simple Pairing has two security goals: protection against passive eavesdropping and protection against man-in-the-middle (MITM) attacks (active eavesdropping). It is a goal of Secure Simple Pairing to exceed the maximum security level provided by the use of a 16 alphanumeric PIN with the pairing algorithm used in Bluetooth Core Specification version 2.0 + EDR and earlier versions. Note that many Bluetooth devices compliant with Bluetooth Core Specification 2.0 + EDR and earlier versions use a 4-digit PIN or a fixed PIN of commonly known values significantly limiting the security on the link.

See, e.g., Bluetooth Core Specification V2.1, 131.

544. The Bluetooth Core Specification also describes implementation of security at both the link layer and the application layer:

1 SECURITY OVERVIEW

Bluetooth wireless technology provides peer-to-peer communications over short distances. In order to provide usage protection and information confidentiality, the system provides security measures both at the application layer and the link layer. These measures are designed to be appropriate for a peer environment. This means that in each device, the authentication and encryption routines are implemented in the same way. Four different entities are used for maintaining security at the link layer: a Bluetooth device address, two secret keys, and a pseudo-random number that shall be regenerated for each new transaction. The four entities and their sizes are summarized in Table 1.1.

Entity	Size
BD_ADDR	48 bits
Private user key, authentication	128 bits
Private user key, encryption configurable length (byte-wise)	8-128 bits
RAND	128 bits

Table 1.1: Entities used in authentication and encryption procedures.

The Bluetooth device address (BD_ADDR) is the 48-bit address. The BD_ADDR can be obtained via user interactions, or, automatically, via an inquiry routine by a device.

The secret keys are derived during initialization and are never disclosed. The encryption key is derived from the authentication key during the authentication process. For the authentication algorithm, the size of the key used is always 128 bits. For the encryption algorithm, the key size may vary between 1 and 16 octets (8 - 128 bits). The size of the encryption key is configurable for two reasons. The first has to do with the many different requirements imposed on cryptographic algorithms in different countries – both with respect to export regulations and official attitudes towards privacy in general. The second reason is to facilitate a future upgrade path for the security without the need of a costly redesign of the algorithms and encryption hardware; increasing the effective key size is the simplest way to combat increased computing power at the opponent side.

See, e.g., Bluetooth Specification V2.1, 1025.

7 SECURE SIMPLE PAIRING

The Secure Simple Pairing security functions and procedures are described in this section. In addition, a cryptographic analysis of each procedure is provided.

There are five phases of Secure Simple Pairing:

- Phase 1: Public key exchange
- Phase 2: Authentication Stage 1
- Phase 3: Authentication Stage 2
- Phase 4: Link key calculation
- Phase 5: LMP Authentication and Encryption

Phases 1, 3, 4 and 5 are the same for all protocols whereas phase 2 (Authentication Stage 1) is different depending on the protocol used. Distributed through these five phases are 13 steps.

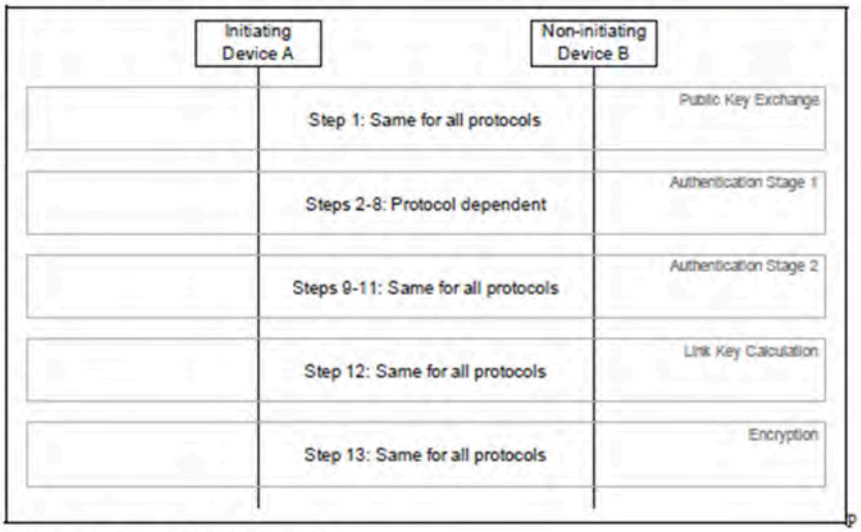


Figure 7.1: Simple Pairing Security Phases

Bluetooth Core Specification, 1058. The Bluetooth core specification describes "Secure Simple Pairing security functions and procedures" between connected devices. In phase 4, "a link key is computed from the derived shared key and the publicly exchanged data" and the "final phase [phase 5] in Simple Pairing is generating the encryption keys." Id., 1067.

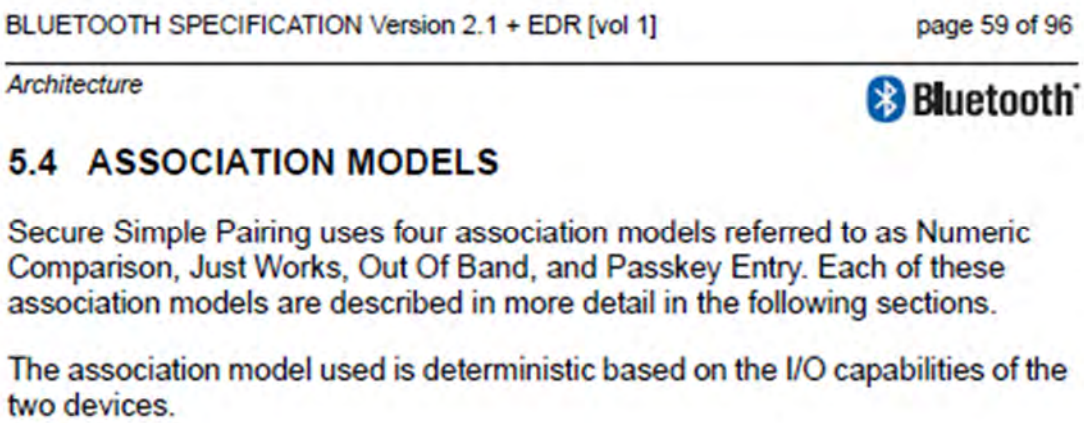
545. Cryptographic authentication between wireless devices like a digital camera and cellular phone was routine at the time of the invention. Id.; Ex. 1017,3 91-92; Ex. 1019, [0055]; Ex. 1020, [0019]. (citing to Bluetooth standards) Indeed, cryptographic authentication was part of the Bluetooth standard for years before the alleged Critical Date. See section V.B.

546. A POSITA would have understood the basic motivation for using cryptographic authentication: to ensure that each device is communicating with its intended recipient and that information is protected from outsiders when transmitted between devices. A POSITA would have found this benefit directly applicable to the system disclosed Kahn, because it would have ensured the secure transmission of image files and related data between the two devices. Kahn teaches that the camera and phone implement a "cableless direct connection" and wireless "detachable connection," a POSITA would have found it obvious to implement Bluetooth as the preferred data transmission mechanism, so there would not have been any unexpected result if the camera and phone were configured to cryptographically authenticate each other.

547. A POSITA would have understood that Bluetooth is the short-range paired wireless connection that comprises the short-range wireless enabled data capture device using an association protocol.

[1.5] wherein establishing the short-range paired wireless connection further comprises the short-range wireless enabled data capture device using an association protocol;

548. The Kahn-Bluetooth combination renders obvious [1.5]. Kahn-Bluetooth teaches or suggests establishing the short-range paired wireless connection further comprises the short-range wireless enabled data capture device using an association protocol. In the combination, the Bluetooth association models would be used, such as the Numeric Comparison model, the Just Works model, the Out of Band model, and the Passkey Entry model. TTI-1019, 133-136.



BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 1] page 59 of 96

Architecture

Bluetooth

5.4 ASSOCIATION MODELS

Secure Simple Pairing uses four association models referred to as Numeric Comparison, Just Works, Out Of Band, and Passkey Entry. Each of these association models are described in more detail in the following sections.

The association model used is deterministic based on the I/O capabilities of the two devices.

See, e.g., Bluetooth Specification V2.1, 133.

5.4.5 Association Model Overview

The following diagram shows Secure Simple Pairing from the point of view of the technology used for discovery and then the different association possibilities.

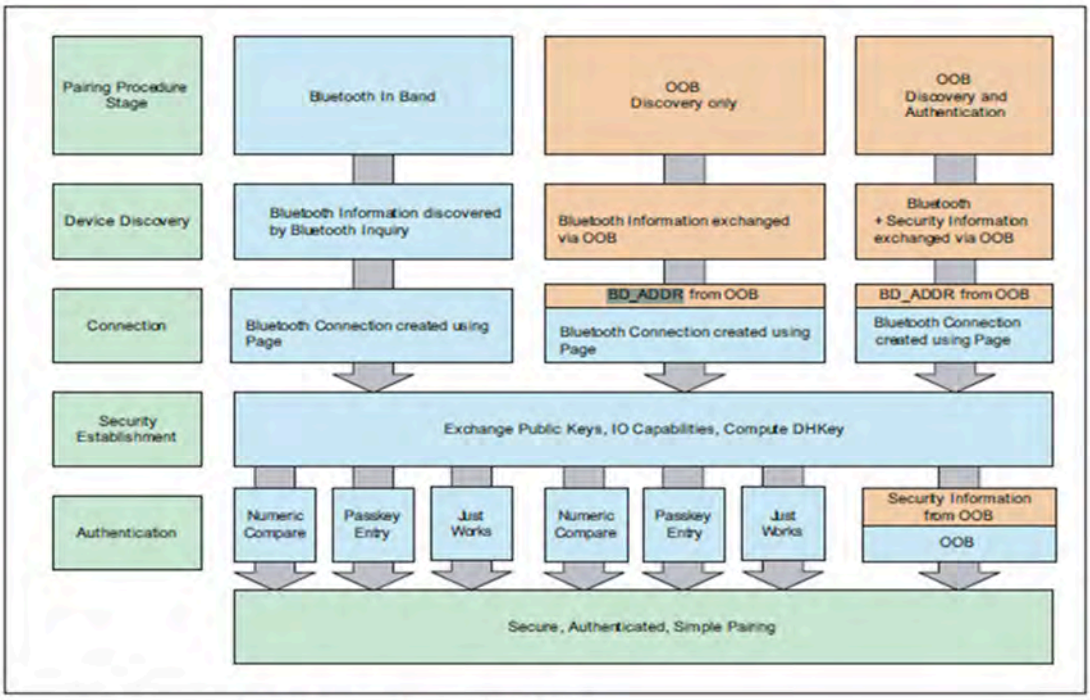


Figure 5.1: Secure Simple Pairing Association Models

See, e.g., Bluetooth Specification V2.1, 135.

[1.6] a data capture circuitry;

549. The Kahn-Bluetooth combination renders obvious [1.6]. Kahn-Bluetooth teaches or suggests a data capture circuitry. For example, Kahn teaches that the camera 100 comprises an "imaging device 120 [which] operates, in essence, by capturing light reflected from the object 150 and transforming that light into image data." Kahn, [0033]-[0035]. Particularly, "the imaging device 120 captures an image of the object 150 via reflected light impacting the image

sensor 230 along optical path 220." Kahn, [0038]. In FIG. 2A, Kahn illustrates "the imaging device 120 compris[ing] a lens 210 having an iris, one or more filter(s) 215 , an image sensor 230 (e.g., CMOS, CCD, or the like), a focus mechanism (e.g., motors) 241, a timing circuit 242 , a signal processor 251 (e.g., analog signal processor), an analog-to-digital (A/D) converter 253 , and an interface 255 ." Kahn, [0037].

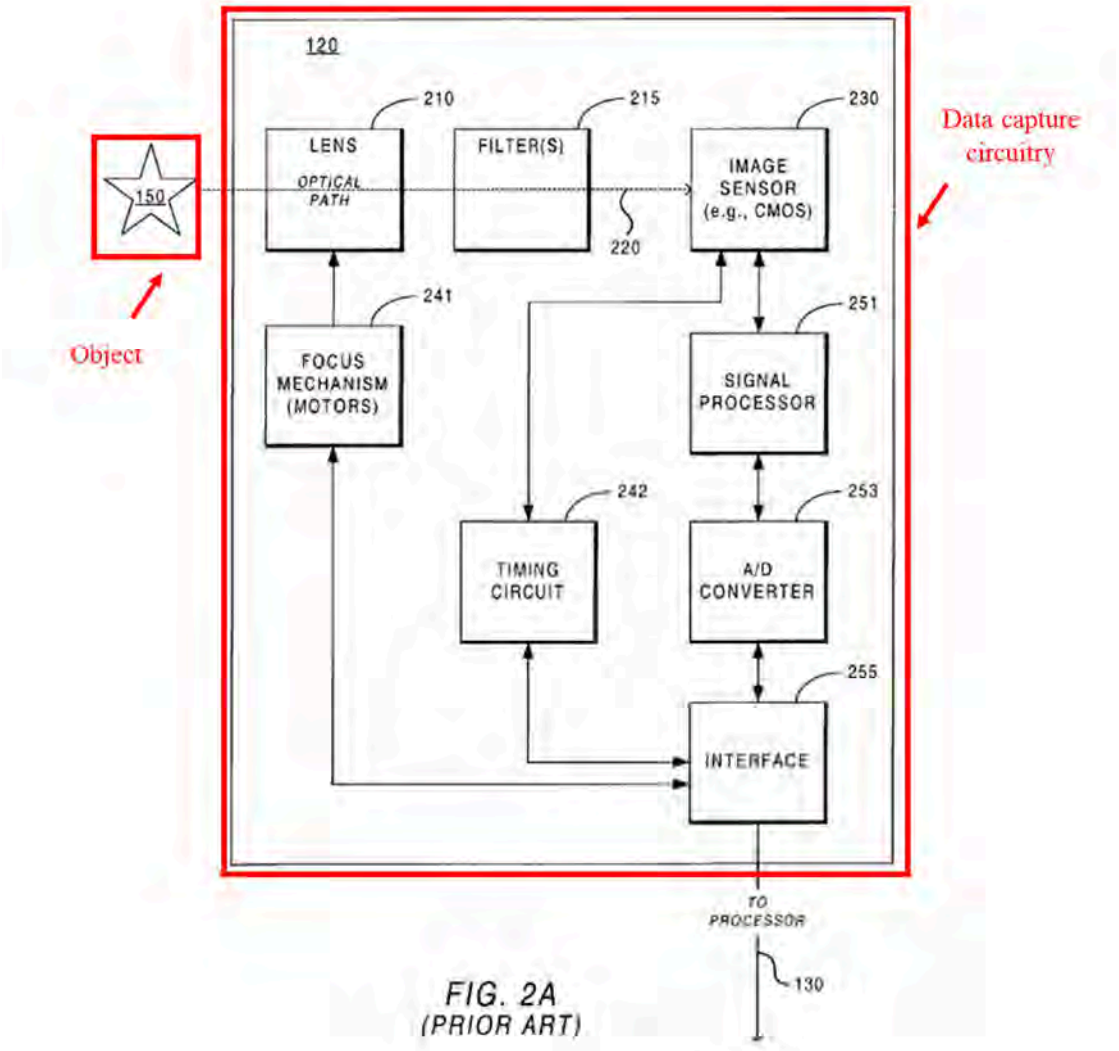


FIG. 2A
(PRIOR ART)

Kahn, FIG. 2A (annotated). Kahn, [0021] ("FIG. 2A is a block diagram of a conventional digital imaging device.").

[1.7] said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry,

550. The Kahn-Bluetooth combination renders obvious [1.7]. Kahn-Bluetooth teaches or suggests said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone. For example, Kahn teaches the computer 140 serves as the central controller for the imaging device 120, directing its actions and timing (Kahn, [0034] ("the computer 140 controls the imaging device 120 by, in effect, telling it what to do and when.")). Through the system bus 130, "the computer 140 [issues] commands [to] the imaging device 120 … to capture an image representing the object 150." Kahn, [0035]. Specifically, Kahn states, "[a] conventional onboard processor or computer 140 is provided for directing the operation of the digital camera 100 and processing image data captured on the imaging device 120." Kahn, [0042]. In FIG. 2B, Kahn illustrates "a block diagram of the processor or computer 140" comprising a dedicated "a processor (CPU) 264," indicating that "[t]he processor (CPU) 264 typically includes a conventional processor device (e.g., microprocessor) for controlling the

operation of camera 100." Kahn, [0042]-[0043]. A POSITA would have understood that the processor 140 is configured to acquire image captured (new-data) by the imaging device 120.

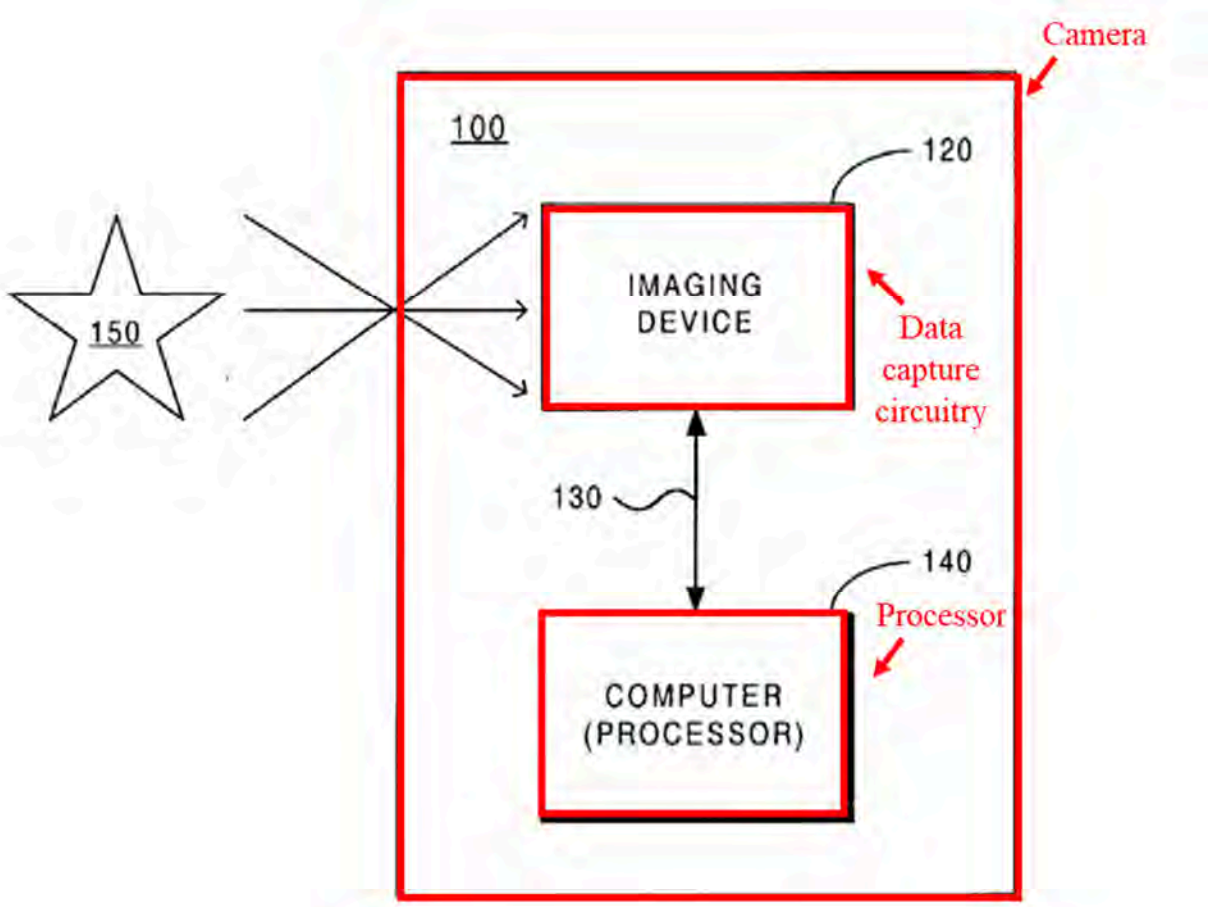
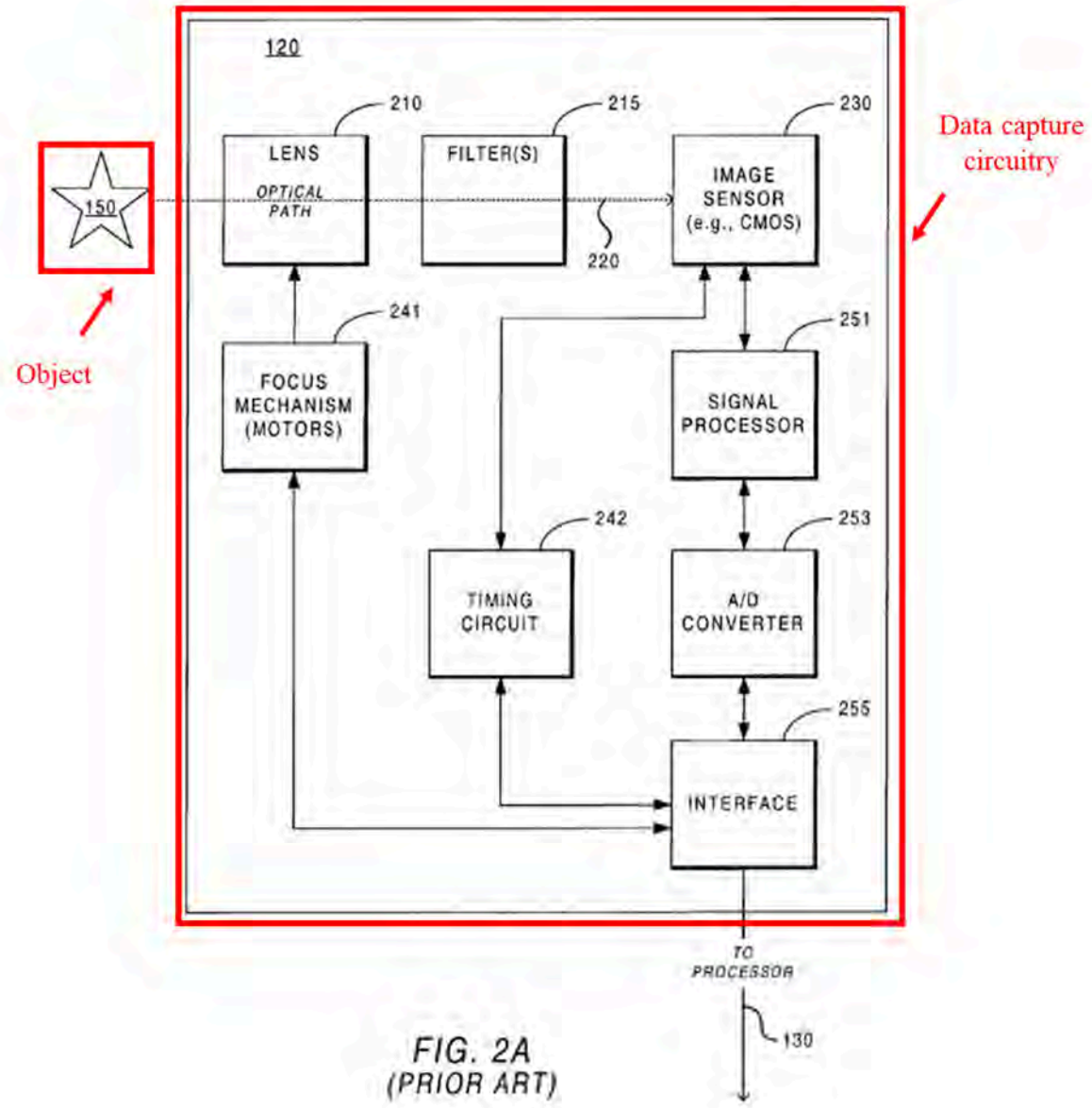


FIG. 1
(PRIOR ART)

Kahn, FIG. 1 (annotated). Kahn, [0020] ("FIG. 1 is a very general block diagram of a digital camera suitable for implementing the present invention.")



Kahn, FIG. 2A (annotated). Kahn, FIG. 2A (annotated). Kahn, [0021] ("FIG. 2A is a block diagram of a conventional digital imaging device.")

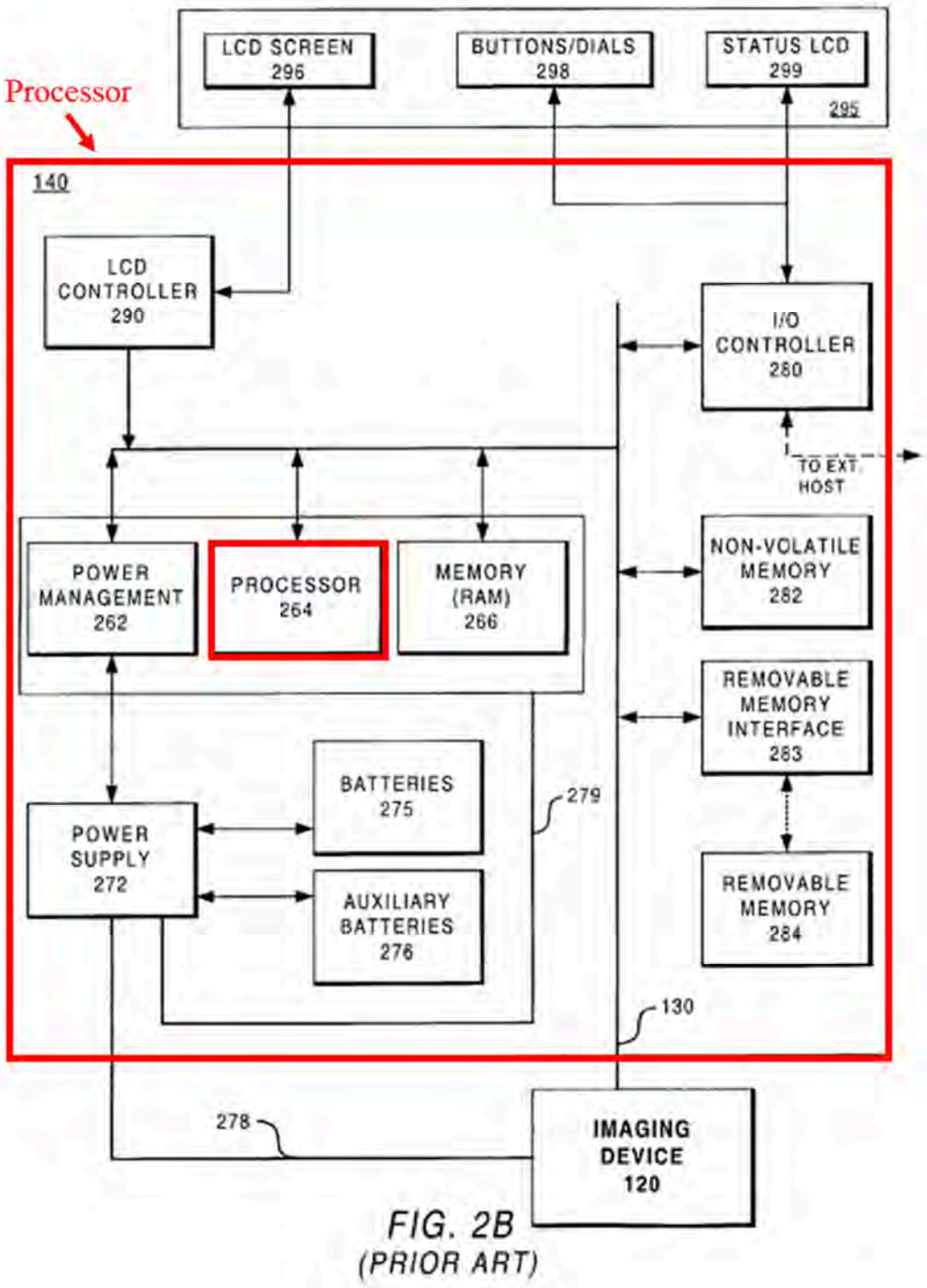


FIG. 2B
(PRIOR ART)

Kahn, FIG. 2B (annotated). Kahn, [0022] ("FIG. 2B is a block diagram of the processor or computer used for the digital imaging device of FIG. 2A.").

[1.8] wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;

551. The Kahn-Bluetooth combination renders obvious [1.8]. Kahn-Bluetooth teaches or suggests the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone. For example, Kahn teaches that "[t]he digital camera 100 may include the user interface 295 for providing feedback to, and receiving input from, a camera user, for example." Kahn, [0046]. Furthermore, Kahn suggests remote operation of the camera, indicating that "these [user interface] elements may be provided through a host device [cell phone] (e.g., personal digital assistant) for a media capture device implemented as a client to a host device." *Id*. A POSITA would have understood that Kahn teaches that a user can remotely operate camera shutter so that object 150 is "captured or recorded as a digital image, upon activation of a shutter mechanism" thus teaching that the new data is acquired after the establishing the short range wireless connection. Kahn, [0033], FIG. 1, 2A-B; *see also, id*., [0007].

552. A POSITA would have been motivated to take pictures after the Bluetooth connection is established so that the pictures could be promptly uploaded to the servers for sharing. TTI-1017, [0086]. Further, there would be no reason to preclude photo capture after the Bluetooth connection is established. On

the contrary, it would be expected that photo capture is always available both before and after the connection to the phone is established. Moreover, Kahn's teaches the association of location data with captured images, and the location information (GPS data) is provided by the phone. Thus, in the combination, the Bluetooth connection between the camera and the phone would be established prior to the capture of images so that the "association of location ID information" may "occur immediately (e.g., upon capture)." Kahn, [0057]-[0058]. Further, Kahn discloses remote operation of the camera via a cell phone, which would have necessitated the establishment of connection before image capture. TTI-1017, [0046]; see also id., [0007], [0033], FIG. 1, 2A-B. Further, Kahn illustrates the continuous checking of the connection between the cell phone and camera as part of the disclosed functionality.

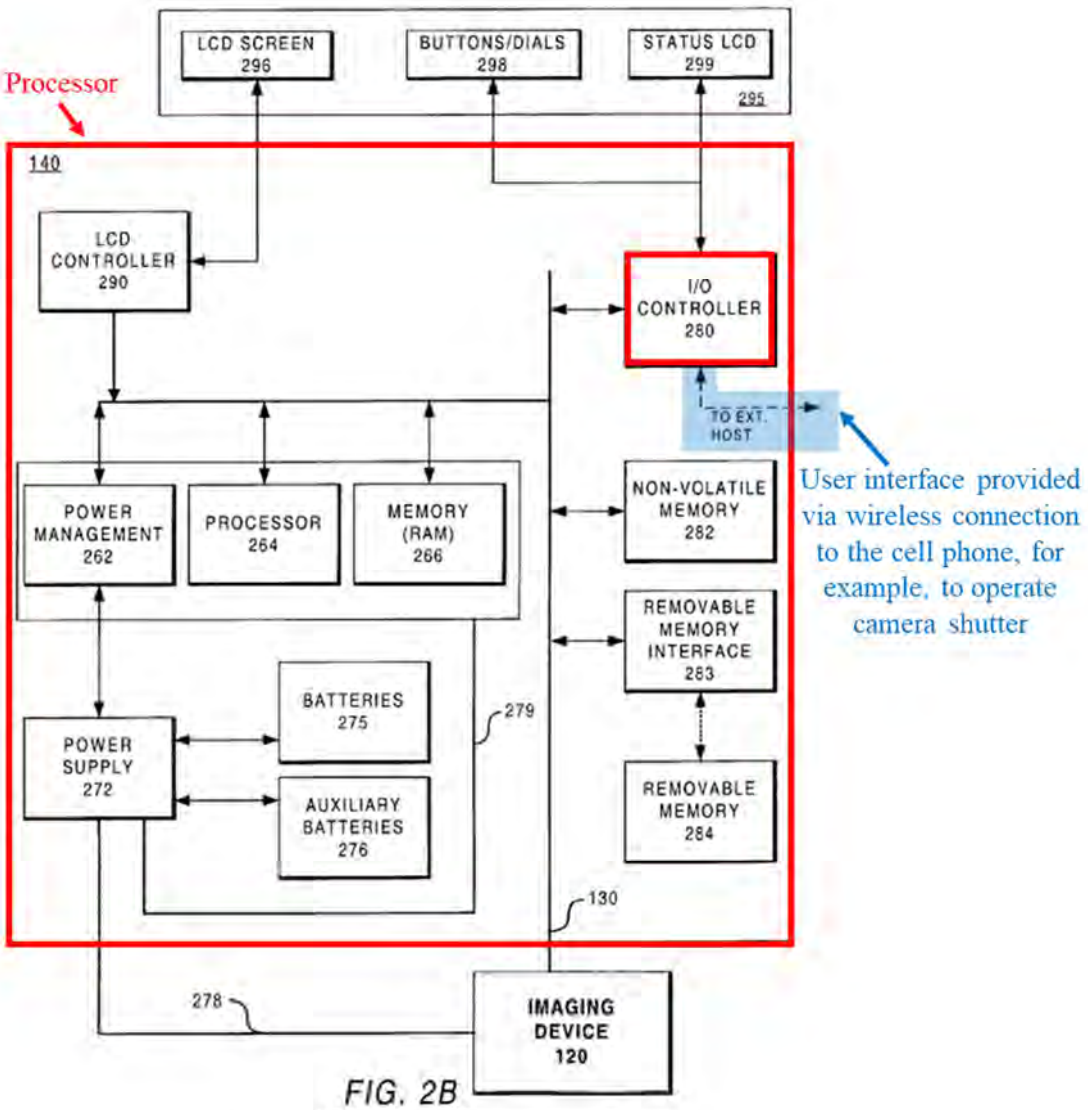


FIG. 2B
(PRIOR ART)

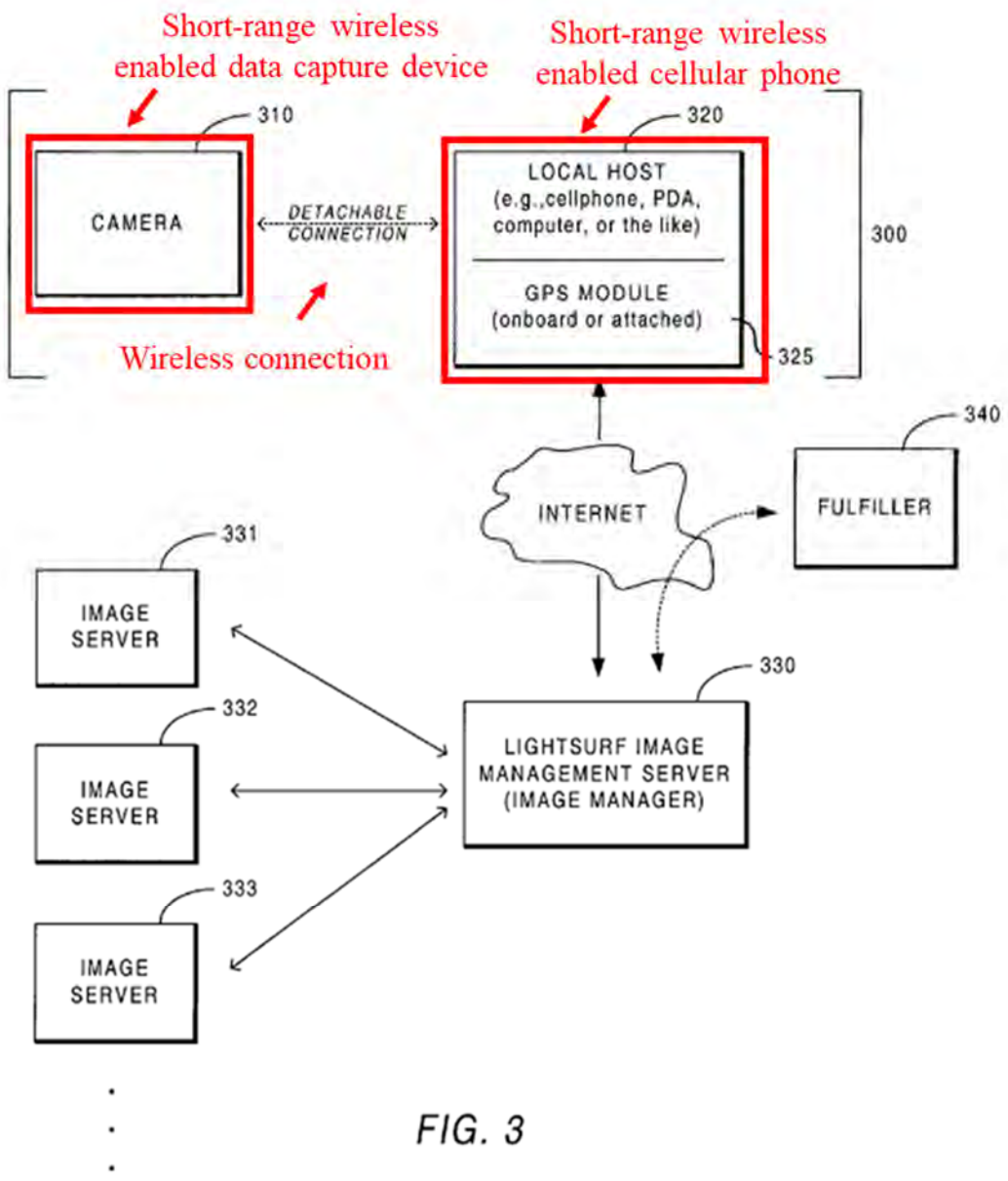


FIG. 3

Kahn, FIG. 3 (annotated). Kahn, [0023] ("FIG. 3 is a high-level block diagram illustrating the basic components that comprise the environment in which the present embodiment may be implemented.")

553. Kahn teaches "the camera device 310 is a stand-alone unit that is occasionally (or persistently) connected to the host device 320, which may be any

device capable of hosting the camera device 310. For example, host device 320 may comprise a cellular phone, a PDA (personal data assistant) with wireless connectivity, or the like. The GPS module 325 is either a stand-alone or integrated module that provides real-time GPS information to the host 320, and in turn to clients of the host (i.e., camera 310) that may submit queries for GPS information." Kahn, [0055]. Thus, a "user employ[ing] the camera 310 to take various pictures (i.e., capture images). Immediately or at some convenient point in time, location ID information (i.e., GPS information) from the GPS module 325 is associated with the images that are captured." Kahn, [0057]. A POSITA would have understood "[t]he association of location ID information (i.e., the GPS-derived longitude and latitude) with one or more images [may] occur[ing] immediately (e.g., upon capture)" is only possible because the camera is connected to the GPS-enabled cell phone when the images are being captured. Kahn, [0058], FIG. 3. Kahn specifies that the camera does not has its own GPS module so the association of the images with GPS information has to occur while the cellular phone is paired with the camera. Kahn, [0058], FIGs. 3, 4.

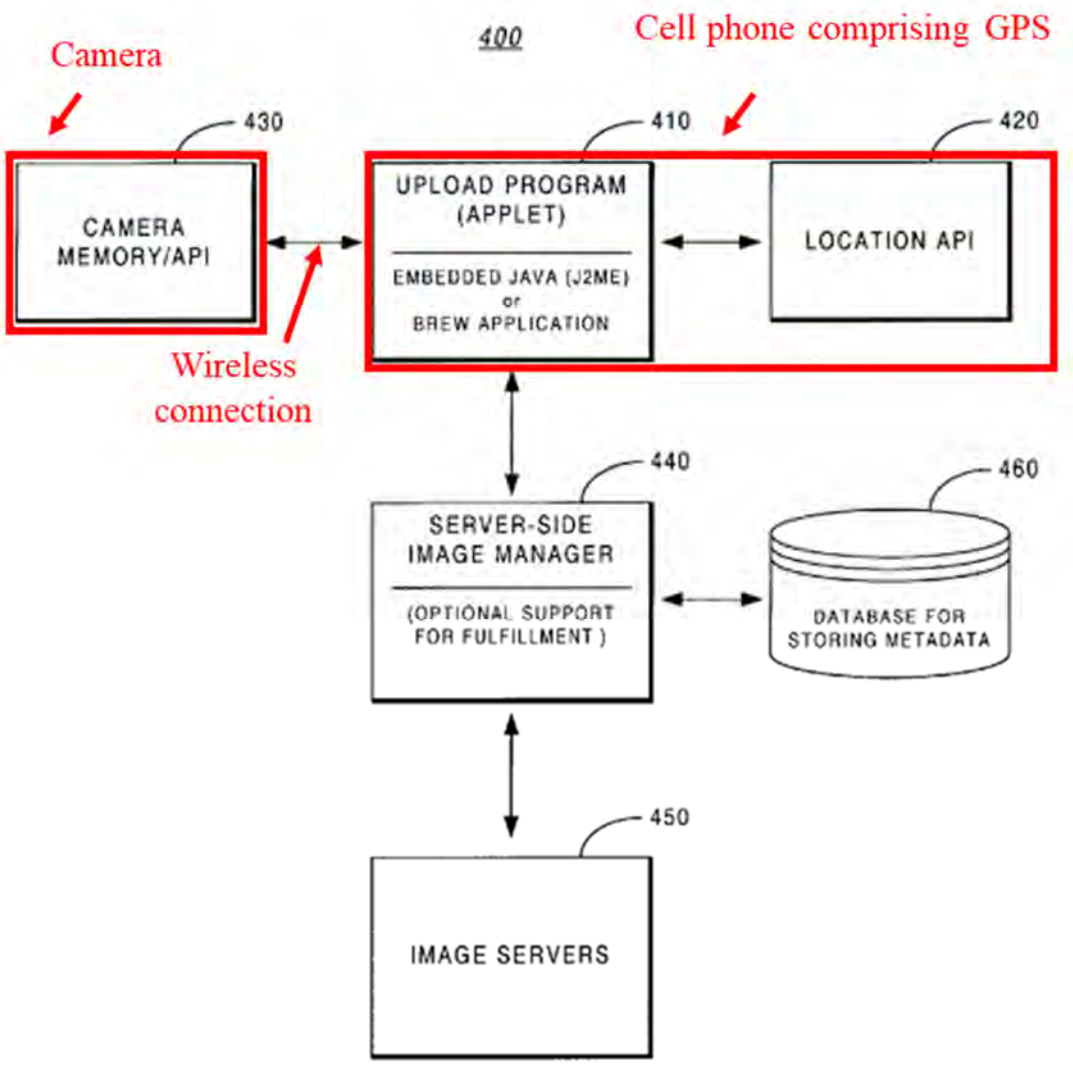


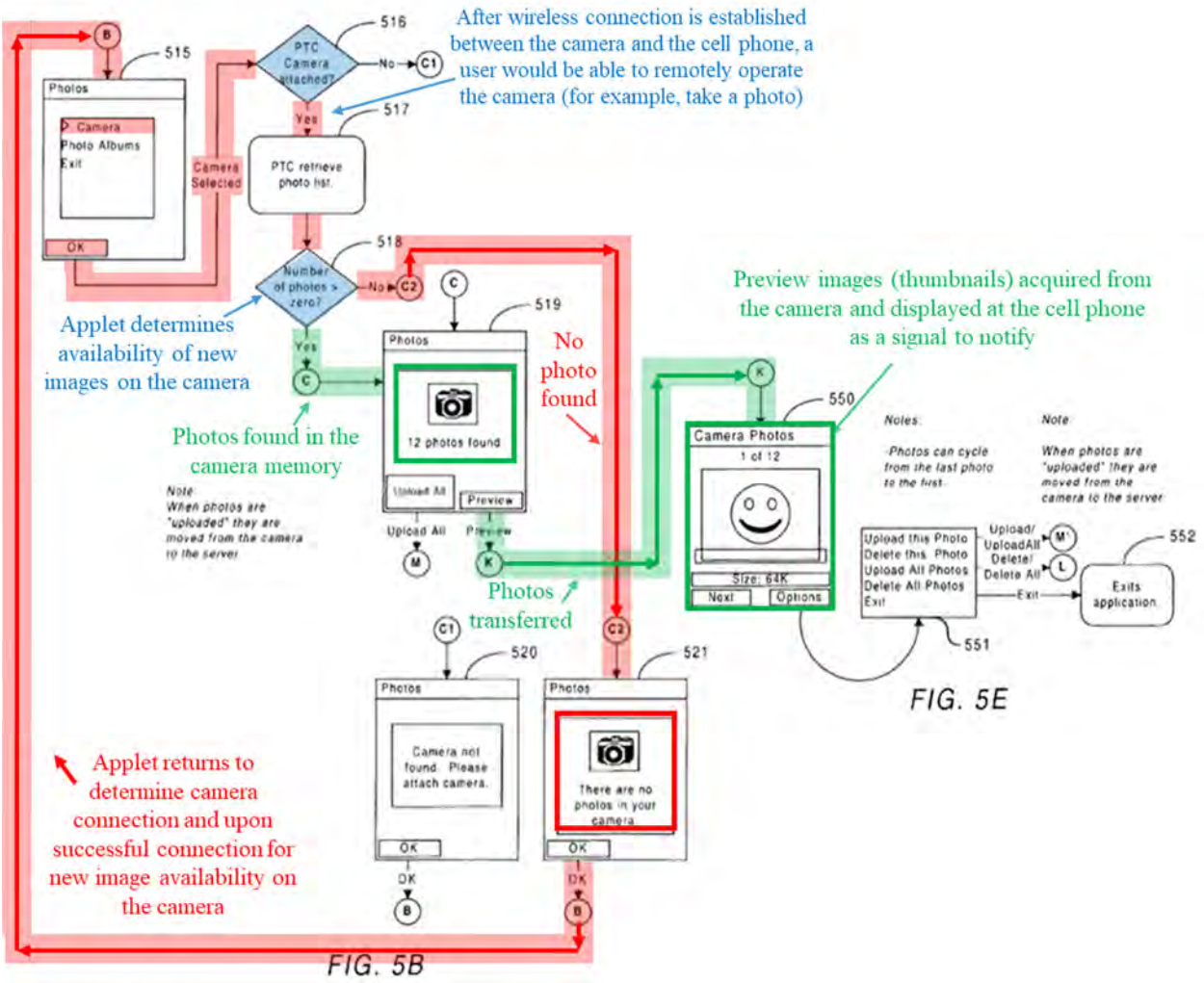
FIG. 4

Kahn, FIG. 4 (annotated). Kahn, [0024] ("FIG. 4 is a block diagram that illustrates implementation of underlying functionality (i.e., processes) in the various modules of FIG. 3.").

554. During the image capturing process, Kahn teaches "location information is automatically captured for individual photographic images

("photos")." Kahn, [0051]. Kahn also teaches that the camera performs "association of location ID information (i.e., the GPS-derived longitude and latitude) with one or more images [may] occur[ing] immediately (e.g., upon capture)" Kahn, [0058]. A POSITA would have recognized that the association of location ID information with images can only occur after the establishment of a short-range paired wireless connection between the data capture device and the cellular phone, as indicated by Kahn's description of the camera device being connected to the host device (e.g., cellular phone) for the association to take place. Kahn, [0055], FIGs. 3, 4. Kahn explicitly states that the GPS module, responsible for providing real-time GPS information to the host device and subsequently associating it with captured images, is either a stand-alone or integrated module connected to the host device, which could be a cellular phone with wireless connectivity. Id. Furthermore, Kahn's description of the upload program communicating with the camera memory/API and the location API, which returns GPS information, underscores the necessity of the camera being connected to the host device to perform the association process. Id., [0062]-[0063], FIGs. 3, 4. Therefore, a POSITA would have understood that the association of location ID information with images is contingent upon the establishment of the short-range paired wireless connection between the data capture device and the cellular phone, as taught by Kahn.

555. Kahn's "FIGS. 5A-F illustrate execution of a client-side embedded applet (i.e., a small footprint application) that executes method steps and displays exemplary user interface (UI) dialogs/menus for supporting fulfillment.", TTI-1017, [0071]. See two examples below of annotated sections of FIG. 5 that show that the phone (client side applet) continuously checks for camera connectivity. In the first example, when the number of photos is non-zero, the "Yes" between flowchart symbols 516 and 517 as part of the (red loop) shows that the phone keeps checking that the camera connection is still active.



Kahn, FIGs. 5B and 5E (partial) (annotated); Figure 5B and 5E of Kahn contemplates a control loop where new pictures are acquired after a connection has been established.

> [0074] Execution path B is employed for uploading photos from the camera. It proceeds as follows. First, the applet displays UI dialog 515, where the user is given access to photos on the camera or on photo albums (e.g., online photos), or the user may simply exit. Of interest for this example is the user selecting "Camera." 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. If the number of photos is greater than zero (tested at step 518), then the applet proceeds to execution path C (below).** If at step 516, the camera is not attached, the applet proceeds to execution path C1 (described below). If at step 518, no photos are found (i.e., the list is empty), the applet proceeds to execution path C2 (described below).
>
> [0075] Execution path C is utilized for displaying a photo uploading UI dialog 519. As shown, the UI dialog 519 indicates the number of photos found. The user may now select to "upload all" photos (execution path M, described below) or simply "preview" photos (execution path K, described below).
>
> [0079] **Execution path K is used for providing the user with an image preview, allowing individual image processing**. At execution path K, **the applet displays UI dialog 550 (FIG. 5E), which allows access to individual images on the camera**. Here, the user is given a variety of options, as indicated by dialog 551: upload this photo, delete this photo, upload all photos, delete all photos, or exit. If the user selects the option to upload the current photo or upload all photos, the applet proceeds down execution path M′. If, however, the user selects the option to delete the current photo or delete all photos, the applet

> proceeds to execution path L. If the user simply selected to "exit" the dialog, the applet terminates execution, as indicated by step 552.

Kahn, [0074]-[0075], [0079] (annotated).

556. Similarly, in the second example that the phone (client side applet) checks for camera connectivity is subsequent to the user's completion of uploading previously acquired photographs can be seen in flowchart symbol 544 in the annotated partial FIG 5 below, where the applet persists in its function to "determine[s] whether the camera is attached [to the cell phone]… [i]f "Yes," the list of photos is retrieved at step 545. Then, at step 546, the applet determines whether the number of photos is greater than zero. If the number is greater than zero, execution proceeds to path K." Kahn, [0086].

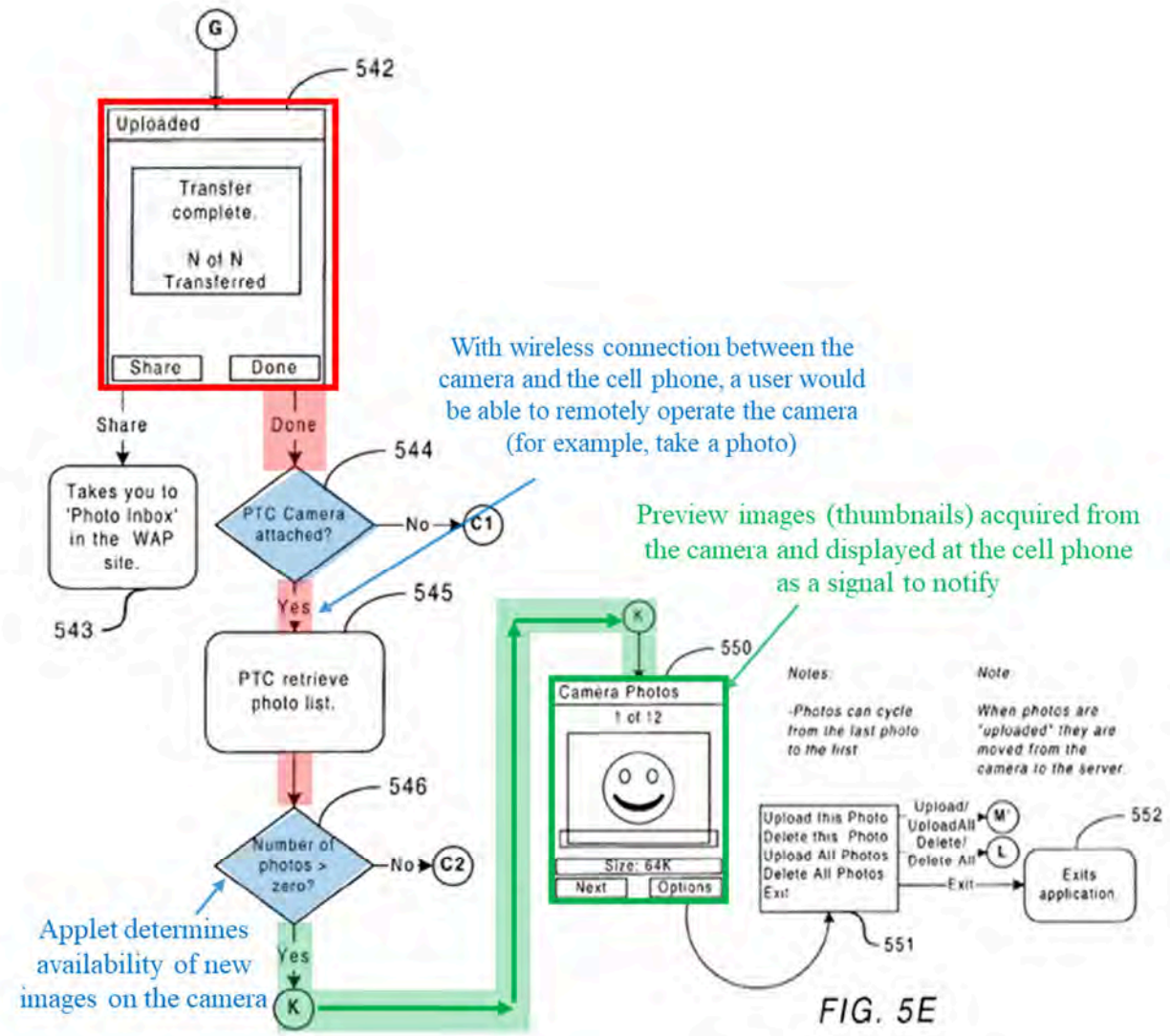


FIG. 5E

FIG. 5D

Kahn, FIGs. 5D and 5E (partial) (annotated).

[0086] Also shown in FIG. 5D, the execution path G proceeds as follows. First, an "uploaded" UI dialog 542 is displayed. Here, the user can select to "Share" the photos, or simply select "Done". In the case where the user has elected to share the photos, execution proceeds to step 543 to take the user to a "Photo Inbox" at the Web site (accessible at the local host via WAP protocol). Otherwise, in the case that the user has elected "Done", execution proceeds to step 544. **At step 544, the applet determines**

> **whether the camera is attached. If not, execution proceeds to path C1. If "Yes," the list of photos is retrieved at step 545. Then, at step 546, the applet determines whether the number of photos is greater than zero. If the number is greater than zero, execution proceeds to path K (described above).** Otherwise, execution proceeds to path C2.
>
> [0079] **Execution path K is used for providing the user with an image preview, allowing individual image processing**. At execution path K, **the applet displays UI dialog 550 (FIG. 5E), which allows access to individual images on the camera**. Here, the user is given a variety of options, as indicated by dialog 551: upload this photo, delete this photo, upload all photos, delete all photos, or exit. If the user selects the option to upload the current photo or upload all photos, the applet proceeds down execution path M′. If, however, the user selects the option to delete the current photo or delete all photos, the applet proceeds to execution path L. If the user simply selected to "exit" the dialog, the applet terminates execution, as indicated by step 552.

Kahn, [0086], [0079]. (Emphasis added.)

557. In the light of the Kahn's teachings, it is evident that Kahn-Bluetooth combination addresses the claimed limitation regarding the processor's configuration to acquire new data in the short-range wireless enabled data capture device using the data capture circuitry. Specifically, Kahn discloses a processor 140 within the digital imaging device 100, serving as the central controller, directing the operation of the imaging device and processing image data captured on it. Kahn further describes the interaction between the processor and the imaging device, where commands are issued to capture images. This aligns with

the concept of acquiring new data using data capture circuitry. Additionally, Kahn teaches remote operation of the camera via a host device, such as a cell phone, which establishes a short-range paired wireless connection, enabling the acquisition of new data after connection establishment. The disclosure illustrates the association of GPS information with captured images, indicating the acquisition of new data post-connection establishment. Kahn also teaches that the connection between the cell phone and camera are checked as part of the disclosed functionality. Therefore, a POSITA would readily recognize that Kahn teaches the processor's configuration to acquire new data through data capture circuitry after establishing a short-range paired wireless connection between the data capture device and the cellular phone.

[1.9] said processor further configured to store the new-data in the memory device;

558. The Kahn-Bluetooth combination renders obvious [1.9]. Kahn-Bluetooth teaches or suggests said processor further configured to store the new-data in the memory device. For example, Kahn teaches "captured image data is transferred over the system bus 130 to the computer 140 which performs various image processing functions on the image data before storing it in its internal memory." Kahn, [0035], [0042].

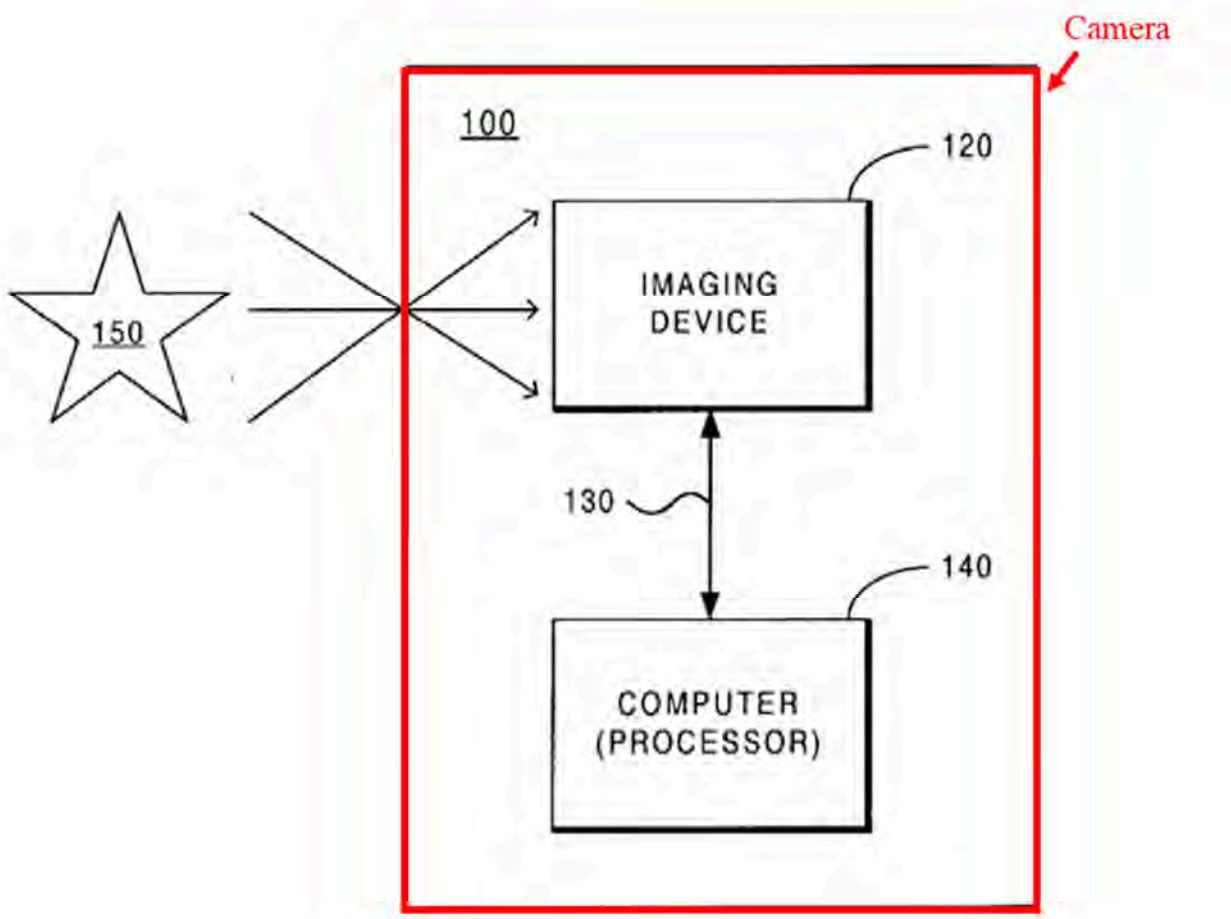


FIG. 1
(PRIOR ART)

Kahn, FIG. 1 (annotated). Kahn, [0020] ("FIG. 1 is a very general block diagram of a digital camera suitable for implementing the present invention.").

559. In FIG. 2B, Kahn illustrates "[a] conventional onboard processor or computer 140 is provided for directing the operation of the digital camera 100 and processing image data captured on the imaging device 120. FIG. 2B is a block diagram of the processor or computer 140. As shown, the system bus 130 provides

connection paths between the imaging device 120, an (optional) power management 262, a processor (CPU) 264, a random-access memory (RAM) 266, an input/output (I/O) controller 280, a non-volatile memory 282, a removable memory interface 283, and a liquid crystal display (LCD) controller 290. Removable memory 284 connects to the system bus 130 via the removable memory interface 283. Alternately, the camera 100 (and therefore the onboard computer 140) may be implemented without the removable memory 284 or the removable memory interface 283." Kahn, [0042].

560. Further, Kahn discloses that "[t]e digital camera 100 includes several memory components. The memory (RAM) 266 is a contiguous block of dynamic memory that may be selectively allocated to various storage functions. Dynamic random-access memory is available from a variety of vendors, including, for instance, Toshiba of Japan, Micron Technology of Boise, ID., Hitachi of Japan, and Samsung Electronics of South Korea. The non-volatile memory 282, which may typically comprise a conventional read-only memory or flash memory, stores a set of computer-readable program instructions to control the operation of the camera 100. The removable memory 284 serves as an additional image data storage area and may include a non-volatile device, readily removable and replaceable by a camera 100 user via the removable memory interface 283. Thus, a user who possesses several removable memories 284 may replace a full removable

memory 284 with an empty removable memory 284 to effectively expand the picture-taking capacity of the camera 100. The removable memory 284 is typically implemented using a flash disk. Available vendors for flash memory include, for example, SanDisk Corporation of Sunnyvale, Calif. and Sony of Japan. Those skilled in the art will appreciate that the digital camera 100 may incorporate other memory configurations and designs that readily accommodate the image capture and processing methodology of the present invention." Kahn, [0044].

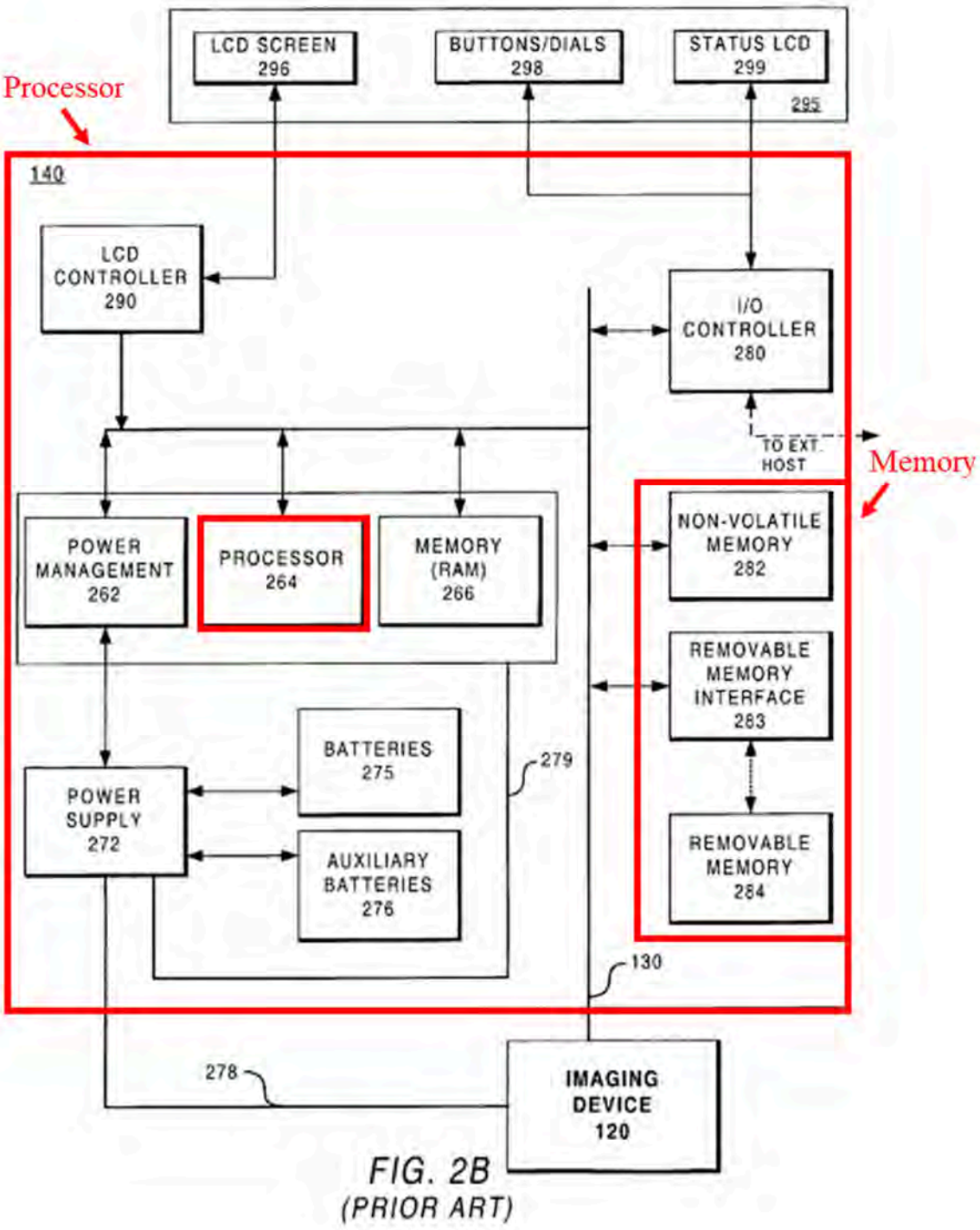


FIG. 2B
(PRIOR ART)

Kahn, FIG. 2B (annotated). Kahn, [0022] ("FIG. 2B is a block diagram of the processor or computer used for the digital imaging device of FIG. 2A.").

561. Kahn discloses a "system 300 [that] includes a camera device 310, a

host device 320, and a GPS (Global Positioning System) module 325. The camera device 310 is preferably a wireless camera device, such as camera device 100 (shown in FIG. 1 A), that either includes wireless connectivity itself or connects to a local host with wireless connectivity." Kahn, [0055], FIGs. 1A, 3.

562. A POSITA would have understood that the processor 254 in the camera device 310 (or camera device 100) will be configured to store captured image data (new-data) in its internal memory (for example, a non-volatile memory 282, a removable memory interface 283, and removable memory 284). Kahn, [0035], [0042].

[1.10] said processor further configured to create a new-data object, wherein the new-data object comprises:

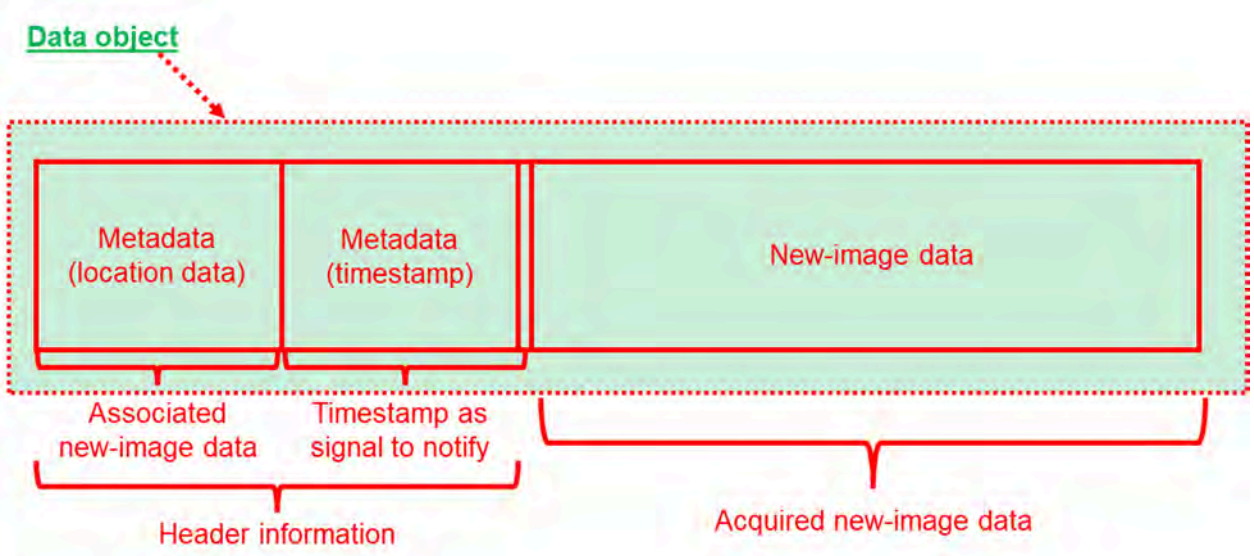
563. The Kahn-Bluetooth combination renders obvious [1.10]. Kahn-Bluetooth teaches or suggests said processor further configured to create a new-data object. For example, Kahn teaches that when an image is captured by the digital camera, the digital camera includes metadata, such as a timestamp in the image file and location ID from a GPS module Kahn, [0057] , [0058] (discussing header information), [0060]. Thus, Kahn teaches the creation of a new-data object that includes acquired new-data (captured images), associated new-data (location ID), and a signal to notify (timestamp).

564. The '030 Patent discloses that "data signal notification is a time-stamp attribute inside the data object wherein the data signal notification corresponds to

existence of new data for transfer, and wherein the time-stamp corresponds to a time when new data was acquired;". TTI-1001, 13:13-21. Kahn teaches that "image data already includes timestamp information (i.e., timestamp indicating when the image is captured)." Kahn, [0060]. Further, Kahn teaches "as images are being uploaded to a destination image server (under control of the image management server), the location ID information may also be conveniently transmitted, either by attaching the information to the image data (e.g., as header information)." Kahn, [0058], [0059].

565. As discussed above (See Ground 2A, [1.5]), Kahn teaches capturing photos (acquiring new-data), for example in step 701 of FIG. 7. During the image capturing process, Kahn also teaches acquiring associated new data such as GPS location information and time stamp information., Kahn, [0058], [0008], [0098].

566. Below is an illustration I made of a new-data object prepared based on the teachings of the Kahn-Bluetooth combination.



567. Furthermore, the GPS location information and timestamp are stored on the phone and uploaded with the full image data. Kahn teaches that metadata associated with the image is being stored in the header of its corresponding image, for example, "the location ID information may be stored together with the image data that comprises the image (e.g., stored in a header)." Kahn, [0059]. Also, Kahn teaches the camera performs "**association of location ID information** (i.e., the GPS-derived longitude and latitude) **with one or more images** [may] **occur[ing] immediately (e.g., upon capture)**" Kahn, [0058]. In addition to GPS information, Kahn also teaches associating timestamp with the image captured. Kahn, [0060] ("the image data already includes timestamp information (i.e., timestamp indicating when the image is captured)"). See also, Kahn, [0008] and [0098].

568. A POSITA would thus understand that the timestamp, full resolution

images, and metadata (location information) are stored on the camera and uploaded to the server through the phone as a data object. Kahn teaches that "[t]he upload program 410 assembles the image data for the images and the corresponding metadata comprising location information and user (identity) information, and then transmits all of that information/data [from the camera to the cell phone and then] to the image management server, via its communication with the server-side application 440 .", [0064]

569. A POSITA would have recognized that the said processor, as described by Kahn, is further configured to create a new-data object based on the captured images and associated location ID information. Kahn, [0051], [0058], [0064]-[0065], [0098]. Kahn's disclosure of the camera device's functionality includes not only capturing photos but also "automatically" associating them with GPS-derived location information immediately upon capture. Id. This association process involves the processor within the camera device, which directs the operation of the imaging device and facilitates the processing of image data. Id., [0034]. Moreover, Kahn's explanation of the upload program's interaction with the camera memory/API and the location API, which returns GPS information, highlights the involvement of the processor in creating a new-data object by associating images with location data. Id.,[0051], [0062]-[0063], FIGs. 3, 4. Since this association occurs as part of the image capturing process facilitated by the

processor, a POSITA would have readily recognized that the processor would have been further configured to create a new-data object comprising images (new-data) associated with location information (associated new-data), as taught by Kahn. Further, when sending data from the camera to the mobile phone, a POSITA would have designed the communication protocol to provide an indication that new photos are available and this indication, whether a time-stamp or otherwise, would be a signal to notify. For example, FIG. 5B notes that "[w]hen photos are 'uploaded' they are moved from the camera to the server." TTI-1017, FIG. 5B. A POSITA would have been motivated to provide, and it would have been obvious to provide, a signal to notify to alert the mobile phone when new images are being received from the camera so that the processor within the camera is notified and can take appropriate action, such as temporarily storing the photos before uploading to a server.

[1.11] 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;

570. The Kahn-Bluetooth combination renders obvious [1.11]. Kahn teaches the inclusion of a timestamp in the image data that is sent from the camera to the mobile phone. Kahn, [0008], [0060], [0098]. Within digital imaging and communication systems, any accompanying data serves as a carrier, conveying essential details about image content and status. A POSITA would have

recognized that leveraging such data as a notification signal for new image availability aligns with established practices in digital communication systems. For instance, Kahn illustrates the inclusion of a timestamp in the image data sent from the camera to the mobile phone. TTI-1017, [0008], [0060], [0098]. In the combination a timestamp would operate as a signal to notify such that when the timestamped data arrives, the processor would read the timestamp and thus be notified that the accompanying data is new data from the camera. TTI-1001, 13:13-21. A POSITA would have observed that the related 8,904,030 patent claims an embodiment in which a "data signal notification is a time-stamp attribute inside the data object." TTI-1001, Claim 6. The same would apply here. TTI-1001, 13:13-21; TTI-1003, 5:14-21.

571. A POSITA would have understood that the timestamp of Kahn was a signal to notify. TTI-1001, 13:13-21. First, the '766 patent does not provide a description of what the signal to notify is; nor does it describe a signal to notify being included in a new data object. Cf., '766 patent, 5:14-21. When trying to ascertain what the signal to notify is, a POSITA would have considered the other patents in the '766 patent family. Specifically, the '030 patent, claim 6 recites, "creating a new data object on the Bluetooth enabled data capture device." '030 patent, cl.6. In the '030 patent, the new data object includes a "data signal notification." Id. Given the very limited disclosure in the '766 patent and '030

patent, and the similarities between the two patents concerning the creation of the new data object, a POSITA would have concluded that the data signal notification of the ’030 patent is the same as the signal to notify in the ’766 patent. TTI-1001, 13:13-21.

572. For example, in the ’766 patent, the signal to notify “corresponds to the acquiring of the new-data for transfer.” E.g., [1.8]. Likewise, in the ’030 patent, the data signal notification “corresponds to existence [sic] of new data for transfer.” ’030 patent, claim 6. Both the signal to notify and the data notification signal use similar terminology and achieve the same results. TTI-1001, 13:13-21. A POSITA would have concluded that the signal to notify in the ’766 patent is the same as the data signal notification in the similarities in the definitions and terminology. TTI-1001, 13:13-21.

573. In the ’030 patent, claim 6, the data notification signal is “time-stamp attribute information inside the data object” where “the time-stamp corresponds to time when new data is acquired.” ’030 patent, claim 6. A POSITA searching the ’766 patent family for an indication of what the signal to notify is would have recognized that the signal to notify includes a time-stamp. TTI-1001, 13:13-21.

574. Kahn teaches capturing photos (acquiring new-data), for example in step 701 of FIG. 7. During the image capturing process, Kahn also teaches acquiring a timestamp and including the timestamp in the image data. *See, e.g.*,

Kahn, [0008], [0060]. Kahn teaches that "the image data already includes timestamp information (i.e., timestamp indicating when the image is captured)." Kahn, [0060]. The timestamp being included with the image data in Kahn satisfies the '766 patent claim limitation of a signal to notify being included in the new data object.

[1.12] the acquired new-data; and

575. The Kahn-Bluetooth combination renders [1.12] obvious. In the combination, Kahn teaches creating a new data object (image data) that includes the image captured by the camera. *See, e.g.*, Kahn, [0007]-[0008], [0058], [0060].

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

576. The Kahn-Bluetooth combination renders obvious [1.13]. In the combination, Kahn teaches that location ID information (associated new-data) is included with the image data. *See, e.g.*, Kahn, [0058].

577. For example, Kahn discloses "automatically" forming metadata associated (associated new-data) with each captured image data. Kahn, [0051], [0057]-[0059], [0062], [0065]. Kahn states that in prior art "imaging devices have only been able to record information about the date/time (timestamp) that an image was captured but not information about the location where the image was captured." Kahn, [0008]. During the uploading process, "[t]he upload program 410 assembles the image data for the images and the corresponding metadata

comprising location information and user (identity) information" Kahn, [0064]. "The metadata … includes fields for user ID, timestamp (date/time), and location ID (longitude and latitude decimal values). Kahn, [0098].

[1.14] 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,

578. The Kahn-Bluetooth combination renders obvious [1.14]. Kahn-Bluetooth teaches or suggests 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. For example, Kahn discloses that "[t]he upload program 410 is implemented as an embedded application in the camera device, the host device, or a combination thereof. …[t]**he upload program 410 is invoked, automatically** … to upload images to the user's account on an image server." Kahn, [0062]. "[T]he upload program 410 also communicates with the camera memory/API 430 , so that the upload program 410 can retrieve images from the camera [internal memory of camera]. In this manner, the upload program 410 is able to invoke [automatic] transfer of the images from the camera to the host (e.g., cell phone), for uploading to a destination image server." Kahn, [0063]-[0064]. See also, Kahn, [0069], [0097].

579. In Figure 7, Kahn illustrates the automatic transfer of images from the

camera to the cell phone and then to the server, detailing the sequential actions involved in this process. TTI-1017, [0063], [0085], FIG. 7. In FIG. 7, Kahn illustrates "a high-level flowchart summarizing a method 700 of operation of the present invention for the automated uploading and organizing of photographic images, based on location information.", "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. At step 703, upon receipt of the request that the images be uploaded, a local application (applet) is invoked that associates location information with the images…Next, the applet transmits this location ID to the image manager, as part of the transmission that uploads the images." Kahn, [0097].

580. The depicted execution paths in FIG. 5D further clarify the automatic transfer process, indicating the initiation of media transfer, verification of data connection, processing of acknowledgment messages, and deletion of photos from local storage upon successful transfer. TTI-1017, [0085], FIG. 5D. For example, Kahn teaches that the new data object goes from the camera, to the cell phone, and then to the server as shown in FIG. 5D, Kahn illustrates automatic "transfer of the

images from the camera to the host (e.g., cell phone), for uploading to a destination image server.”, Kahn, [0063]. Kahn specifies automatic transfer using Execution path HI, outlined in FIG. 5D, which entails several sequential actions. Kahn, [0085]. Initially, at step 536, the applet initiates a media transfer by sending a corresponding message. Kahn, [0085]. Subsequently, at step 537, the applet verifies the presence of a valid data connection. If such a connection exists, the execution progresses to step 538, where the applet proceeds to process a media transfer acknowledgment message. Kahn, [0085]. However, in the event of an unsuccessful acknowledgment (step 539), execution diverts to path F, directing to dialog 531. Kahn, [0085]. Conversely, upon a successful acknowledgment, the applet proceeds to step 540, wherein it deletes the photo from local storage. Kahn, [0085]. Following this, at step 541, the applet evaluates whether additional photos necessitate transfer. If affirmative, the execution loops back to step 536 to commence the process anew. Kahn, [0085].

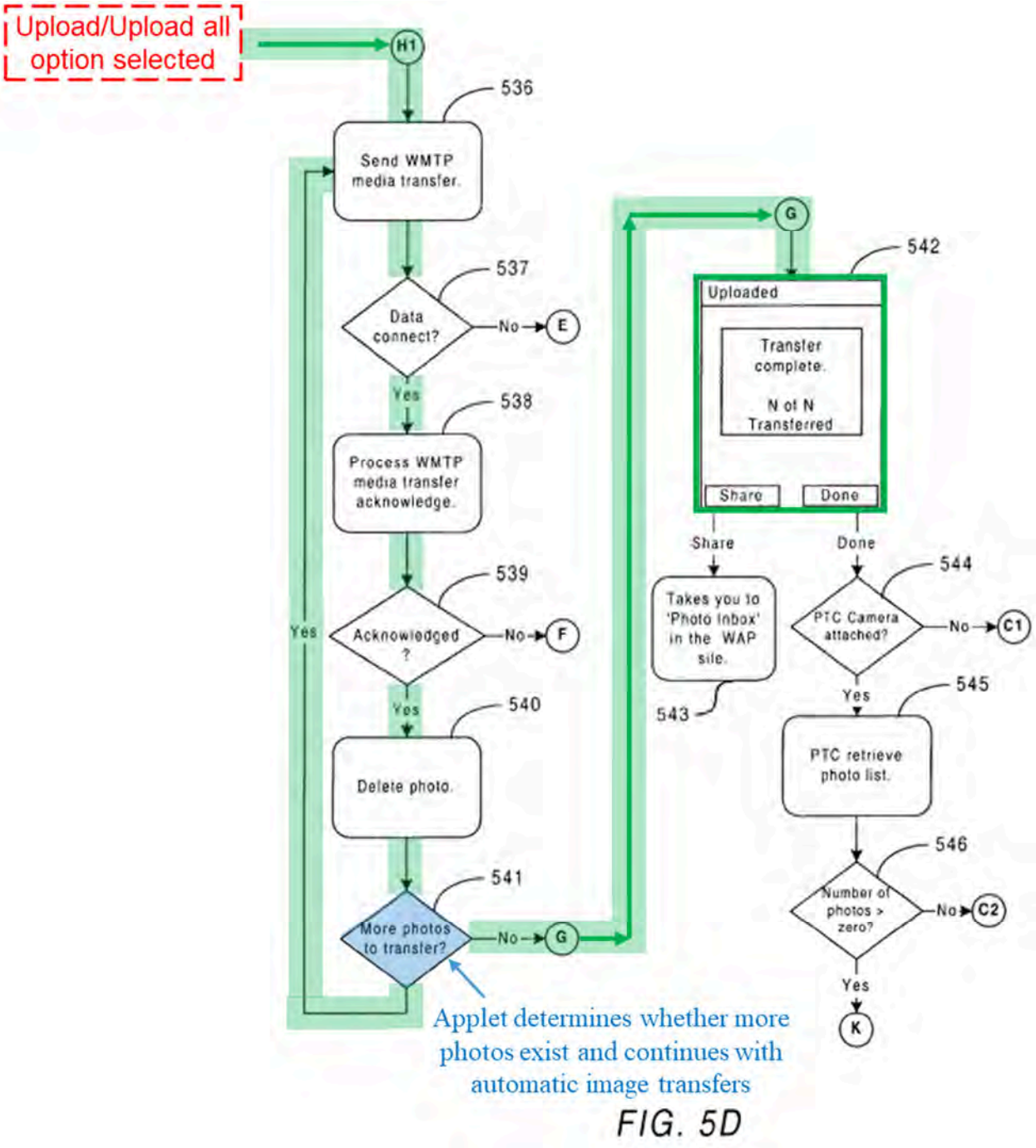
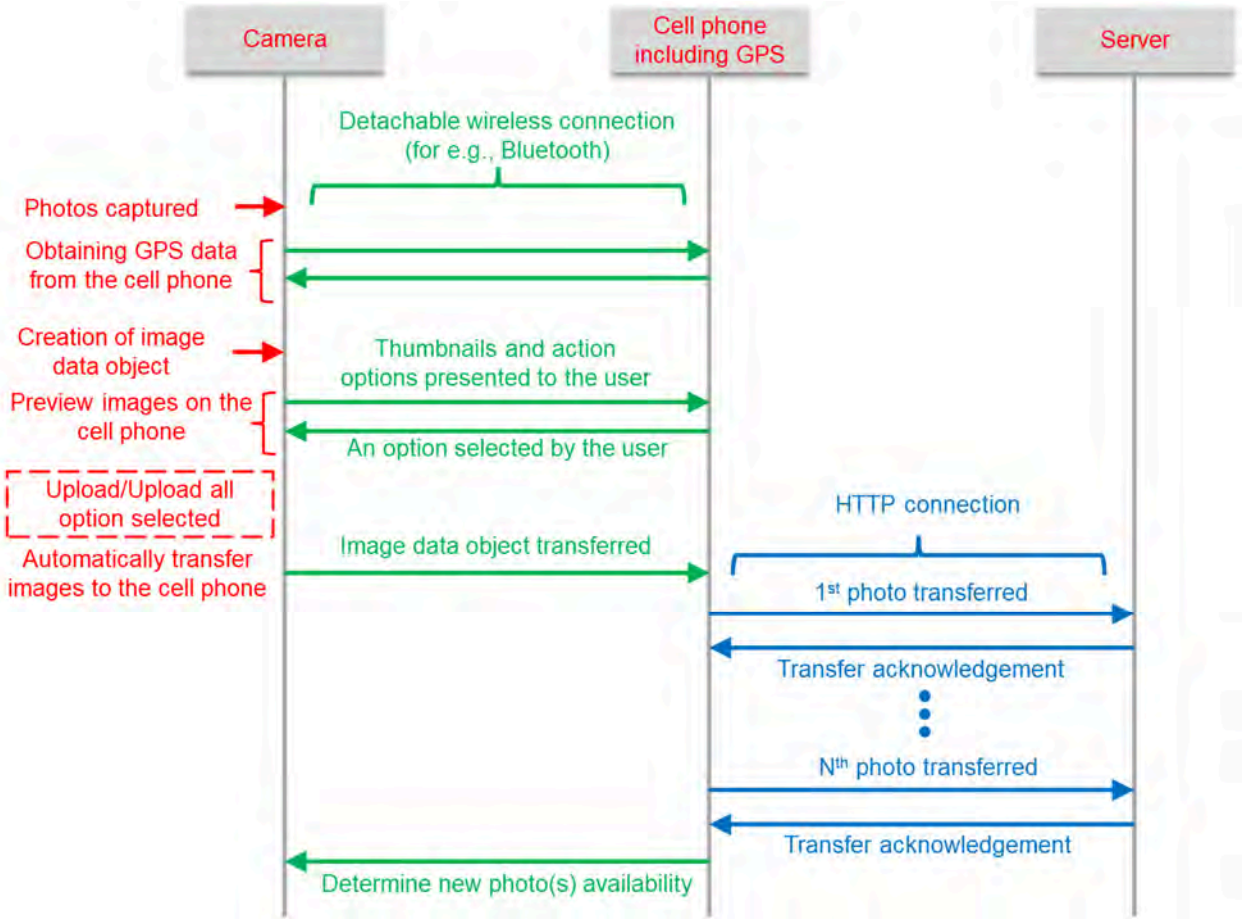


FIG. 5D

Kahn, FIG. 5D (annotated)

581. Referring the Kahn-Bluetooth combination, wee an illustration below that I made indicating one dataflow that would be implemented between a camera, a local host (e.g., cell phone) and an online Web-based image management server

330 based on the teachings of Kahn is depicted.



582. Thus, based on Kahn's teachings, it is evident that the camera's processor is configured to transfer automatically the new-data object to the cellular phone over the established short-range paired wireless connection.

[1.15] 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,

583. The Kahn-Bluetooth combination renders obvious [1.15]. Kahn-Bluetooth teaches or suggests 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. See Ground 2A, [1.7]. For example, Kahn discloses "the 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." Kahn, [0057]. Kahn discloses that cell phone "applet proceeds to step 516 to determine whether the camera is currently attached. If "Yes," a list of photos is retrieved at step 517. If the number of photos is greater than zero (tested at step 518)" Kahn, [0074], FIG 5B. A POSITA would have understood that this functionality of consistently monitoring availability of new images on the camera would constitute as listening to the notification signal about new images acquired by the camera. Furthermore, as discussed previously (see Ground 2A, [1.7], [1.14]), the Kahn-Bluetooth combination discloses the cell phone being configured to receive the new-data object because Kahn teaches that the new data object goes from the camera, to the cell phone, and then to the server. As shown in FIG. 5D, Kahn illustrates automatic "transfer of the images from the camera to the host (e.g., cell phone), for uploading to a destination image server.", Kahn, [0063]. Therefore, based on Kahn's teachings, in the combination, the cell phone would use something in the data object, such as a timestamp or a portion of the header, and would read such information to detect when a signal to notify has arrived. As such, the cellular phone is configured to listen to the signal to notify

and received the new-data object, such as new photos from the camera.

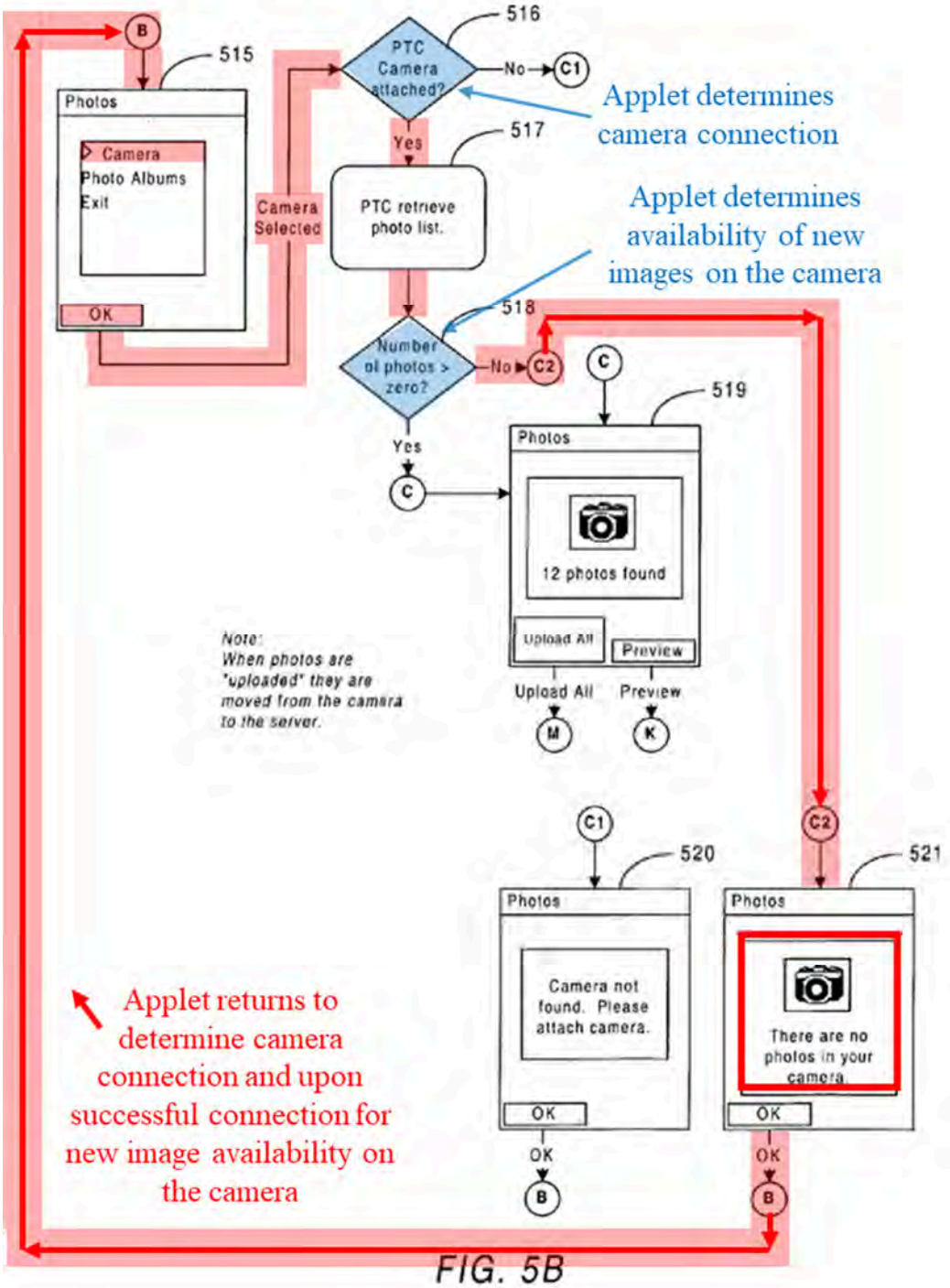
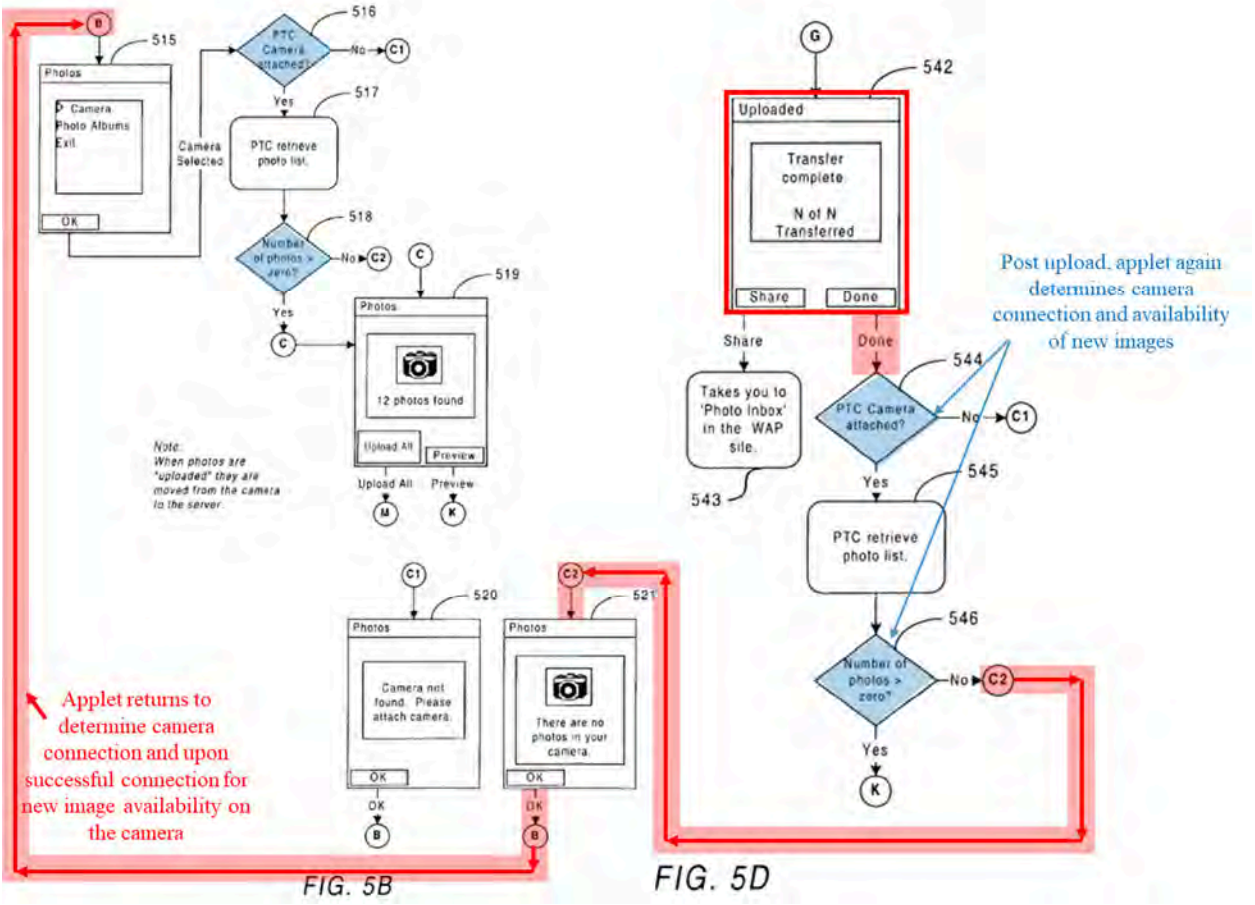


FIG. 5B

Kahn, FIG. 5B (annotated). A POSITA would have recognized that cell phone determining number of photos available on a camera would constitute as listening. Kahn, [0074], [0076], FIG. 5B.



Kahn, FIG. 5B and 5D (partial) (annotated). Post uploading of photos to the server (refer figure element 546 in FIG. 5D), Kahn teaches that the cell phone once again determines number of photos available on a camera would constitute as listening. Kahn, [0074], [0076], FIG. 5B. As discussed above (See Ground 2A, [1.10] and [1.12]), Kahn discloses cell phone configured to receive new-data object.

[1.16.1] wherein a mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the signal to notify

584. The Kahn-Bluetooth combination renders obvious [1.16.1]. Kahn-Bluetooth teaches or suggests wherein a mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the signal to notify. As discussed above (See Ground 2A, [1.3]), Kahn teaches that the camera 310 is wirelessly connected with the local host 320 (for example, a cell phone) . Kahn, [0055], FIG. 3. Kahn teaches "the client-side applet program, which may be embodied as an embedded J2ME applet in the local host" for example a cell phone. Kahn, [0071], [0055]. Kahn teaches that "a client-side embedded applet (i.e., a small footprint application) [that] executes method steps and displays exemplary user interface (UI) dialogs/menus for supporting fulfillment." Kahn, [0071]. Accordingly, the applet performs different functions, for example, "applet determines whether the camera is currently connected to the local host [for e.g., cell phone]", "applet determines whether the number of photos is greater than zero", "applet displays UI menu," "applet establishes a connection to the photo site (Web-based server providing image management) for uploading of photos." Kahn, [0070]-[0086], FIGs. 5A-5F.

585. As discussed above (See Ground 2A, [1.7]-[1.11]), the camera creates a new-data object to be transferred to the image server via cell phone that includes

thumbnails, metadata associated with the image and the image data captured by the camera. In some instances, Kahn refers to "a client-side embedded applet" as an "upload program". Kahn, [0062], FIG. 4. A POSITA would have understood that the upload program and the applet are interchangeably used because the upload program (similar to applet) "would be embedded as an application in a device run-time environment, such as J2ME (Sun Microsystems) or BREW (QUALCOMM)." Kahn, [0062].

586. Kahn teaches, "the upload program 410 [also] communicates with the camera memory/API 430, so that the upload program 410 can retrieve images from the camera." Kahn, [0063]. A POSITA would have understood that while images from the camera, the upload program also retrieves the associated image data (for example, metadata, thumbnail). Subsequently, at the cell phone, the "upload program 410 assembles the image data for the images and the corresponding metadata comprising location information and user (identity) information." Kahn, [0064]. Further, the upload program "establishes an Internet connection to the server, for example, using HTTP protocol," Kahn, [0056]. The applet is then responsible for "transmit[ting] all of that [assembled] information/data to the image management server, via its communication with the server-side application 440." Kahn, [0064].

587. A POSITA would have understood that assembling the image data

would constitute processing of image data images from the camera would involve processing the received new-data object in accordance with the HTTP so that the data object can be transmitted over the internet. Kahn, [0064]. Therefore, a POSITA would have understood that the applet, through its processing of image data and establishment of internet connections, effectively processes the signal to notify, in the combination, because the applet takes the foregoing actions in response to the signal to notify, and the act of responding to the signal to notify constitutes "processing" of the signal to notify.

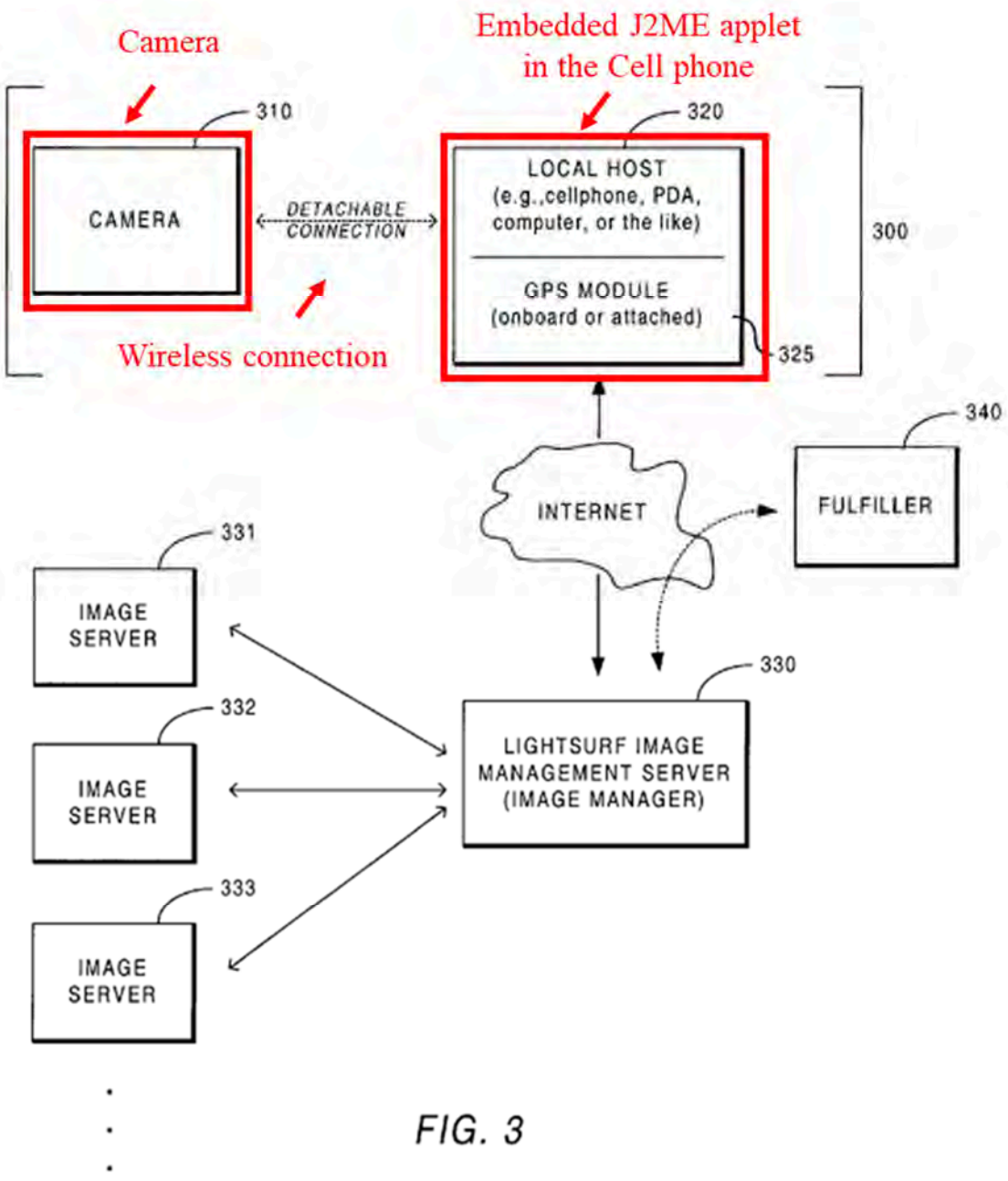


FIG. 3

Kahn, FIG. 3 (annotated).

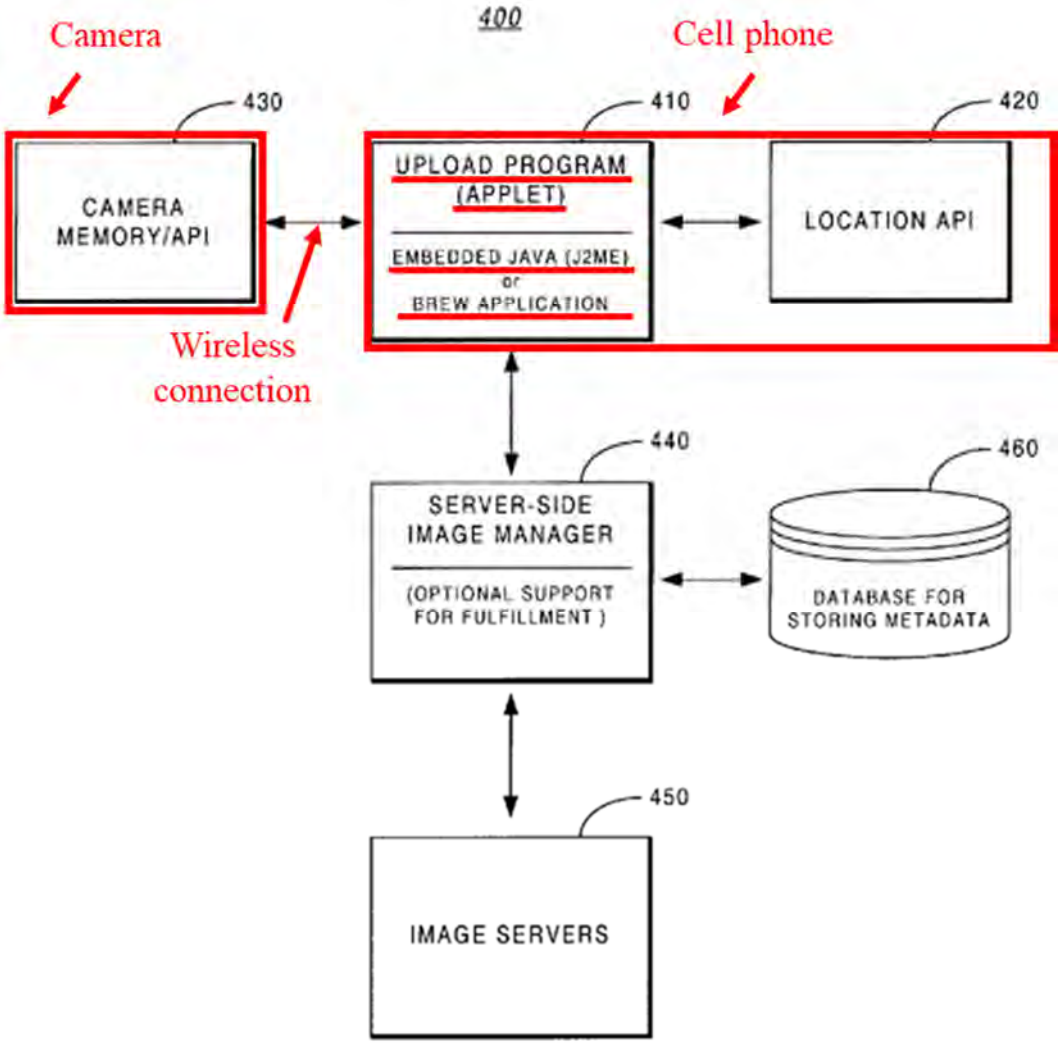


FIG. 4

Kahn, FIG. 4 (annotated).

[1.16.2] and store the received new-data in a memory device of the cryptographically authenticated short-range wireless enabled cellular phone,

588. The Kahn-Bluetooth combination renders obvious [1.16.2]. Kahn-Bluetooth teaches or suggests to store the received new-data in a memory device of the cryptographically authenticated short-range wireless enabled cellular phone.

During uploading process, Kahn teaches "transfer[ing] of the images from the camera to the host (e.g., cell phone), for uploading to a destination image server." Kahn, [0063]. Kahn also teaches that once a photo is uploaded to the server, the applet deletes the photo from the cell phone's memory (local storage). Kahn, [0085] ("step 540, where the photo is deleted (from local storage)."), FIG. 5D (figure element 540). Thus, a POSITA would have understood that in order to delete the photo from the cell phone's memory the photo would have been stored in the first place. The photos thus must have been stored at least temporarily in the cell phone's memory before its deletion.

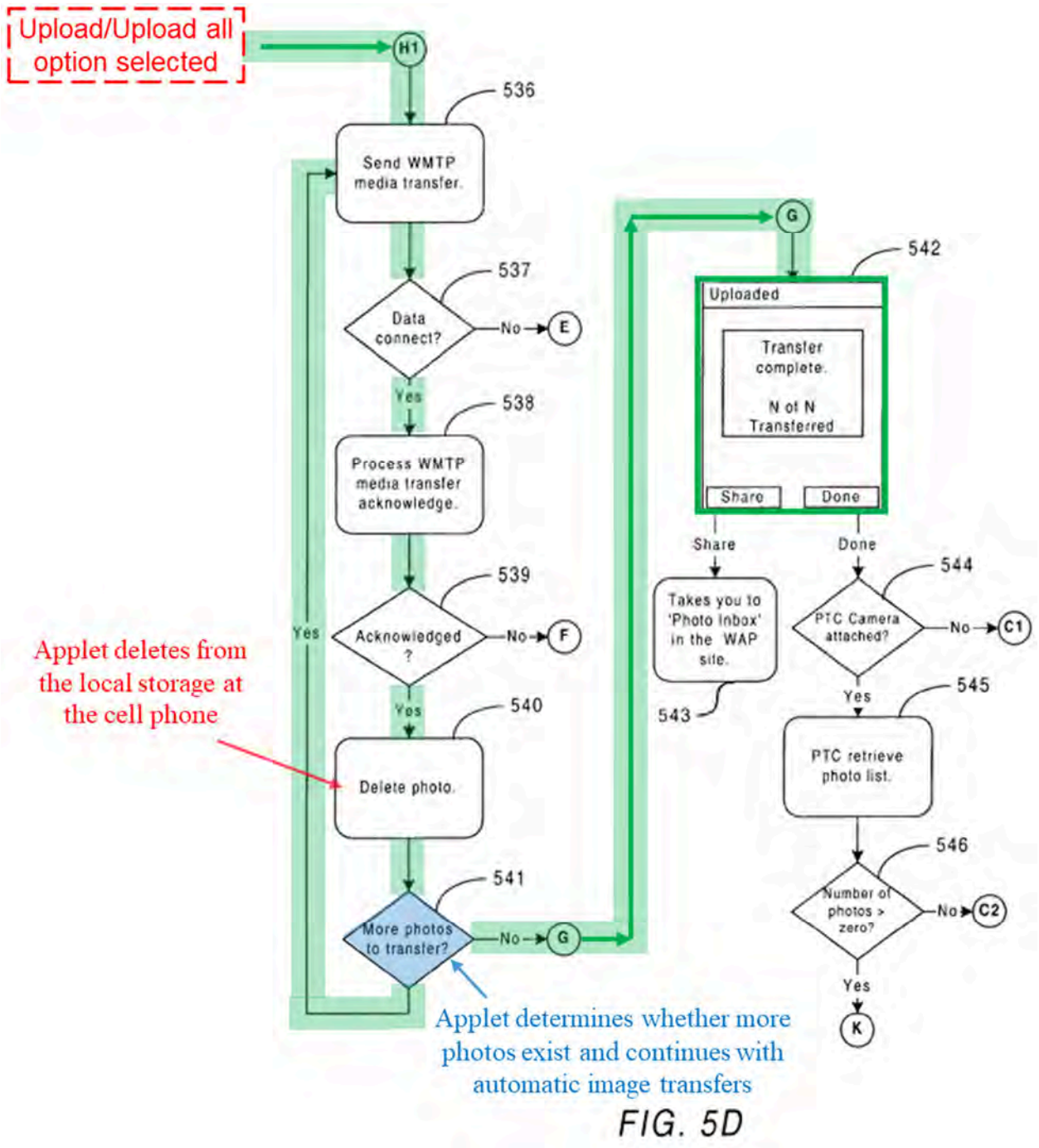


FIG. 5D

Kahn, FIG. 5D (annotated).

[1.17] 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

589. The Kahn-Bluetooth combination renders obvious [1.17]. Kahn-Bluetooth teaches or suggests 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. Kahn teaches utilization of HTTP protocol by the host device to establish an internet connection with the image management server, facilitating the uploading of data to the website. TTI-1017, [0056] ("the host device 320 communicates with an online Web-based image management server 330. … the image management server 330 is a Web-based server accessible via the Internet … [i]n order to communicate with the image management server 330, the host device 320 establishes an Internet connection to the server, for example, using HTTP protocol.") Kahn outlines the functionality of the image management server, allowing the system to organize images into online albums accessible to users through web browser software. TTI-1017, [0063]-[0065]. For example, Kahn teaches the image management server "allows the system to place images into an online or digital photo album … [s]uch albums may then be accessed by the user (and shared with other users) using Web browser software (e.g., Microsoft Internet Explorer)." Kahn, [0063]-[0065]. "Upon receipt of the transmission from the applet, the image manager proceeds to store the images (in an image server) and stores the location ID information in the

metadata database." TTI-1017, [0098]. The database stores a "user ID," "timestamp," and "location ID." Id. In the combination, a POSITA would have provided the user ID information along with the photo and metadata so that the web-based server would know who the photo is associated with. Even though a user may have logged into the web-based server with the user ID and password, and thus the server is aware of the user ID, a POSITA would have understood that for privacy and security, it would have been advantageous to further send the user ID along with the new data as a redundant safeguard. TTI-1017, [0071]-[0073], [0082].

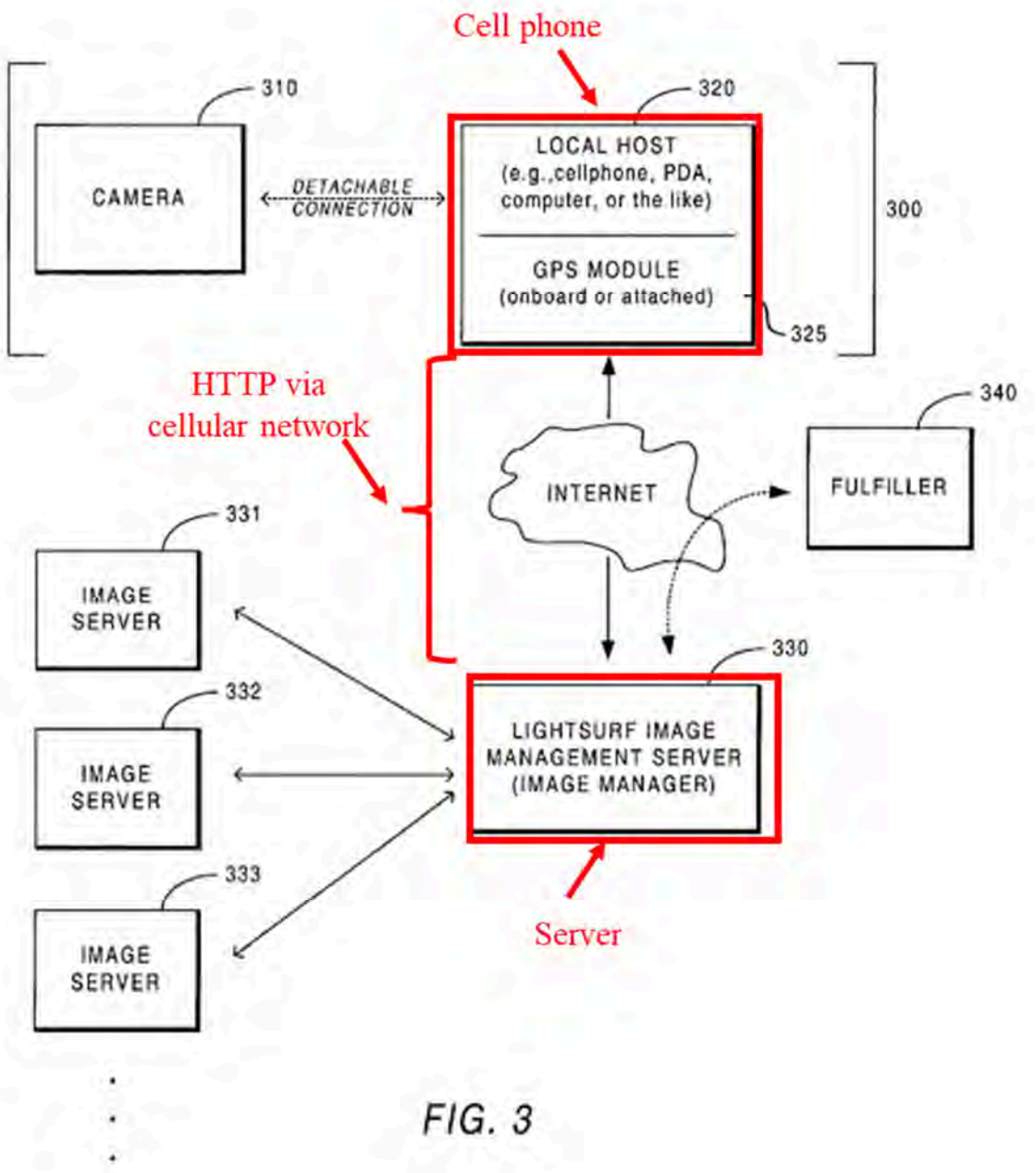


FIG. 3

FIG. 3 (annotated). Kahn, [0023] ("FIG. 3 is a high-level block diagram illustrating the basic components that comprise the environment in which the present embodiment may be implemented.")

[1.18] 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.

590. The Kahn-Bluetooth combination renders obvious [1.18]. Kahn-Bluetooth teaches or suggests 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. For example, Kahn teaches "[t]he upload program 410 assembles the image data for the images and the corresponding metadata comprising location information and user (identity) information" and then "transmits all of that information/data to the image management server." Kahn, [0063]-[0064]. Kahn also teaches "[t]he 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)." Kahn, [0098] (emphasis added.) A POSITA would have understood that this user information included in the metadata is integral to the operation of the user data publishing website, as it uniquely identifies a particular user. Kahn, [0063], [0098].

591. Kahn also teaches that system is configured "place images into an online or digital photo album." Kahn, [0065]. Additionally, Kahn specifies that a "user is given access to photos on the camera or on photo albums (e.g., online

photos)." Kahn, [0074]. However, this access is contingent upon the validity of the user credentials. Kahn, [0082], [0084], FIG. 5A, 5C (elements 522, 526) . For example, Kahn discloses that "the applet [at the cell phone] retrieves the NAI and password" from the cell phone's memory and transmits the login credentials "to the photo site (Web-based server providing image management)" to determine the validity of the user credentials. Kahn, [0082]. The NAI acts as a user ID and may be, for example, a cell phone number. Id., [0071]. To serve as a network access identifier, the NAI would uniquely identify a user of the desired data publishing website.

592. Post-upload, Kahn teaches that the user is provided with an option to either "share" or keep the album private, and thus in the combination, photos may be published to the photo website for private consumption. Kahn, [0086] ("the user can select to "Share" the photos, or simply select "Done""), FIG. 5D (figure element 542). Moreover, Kahn teaches that publication of "[s]uch albums may then be accessed by the user (and shared with other users) using Web browser software (e.g., Microsoft Internet Explorer)." Kahn, [0065]. In light of Kahn's teachings, it would be evident to a POSITA that without sharing the albums not shared would be exclusively available for private consumption on the user's account on the website. Kahn, [0086], FIG. 5D (figure element 542).

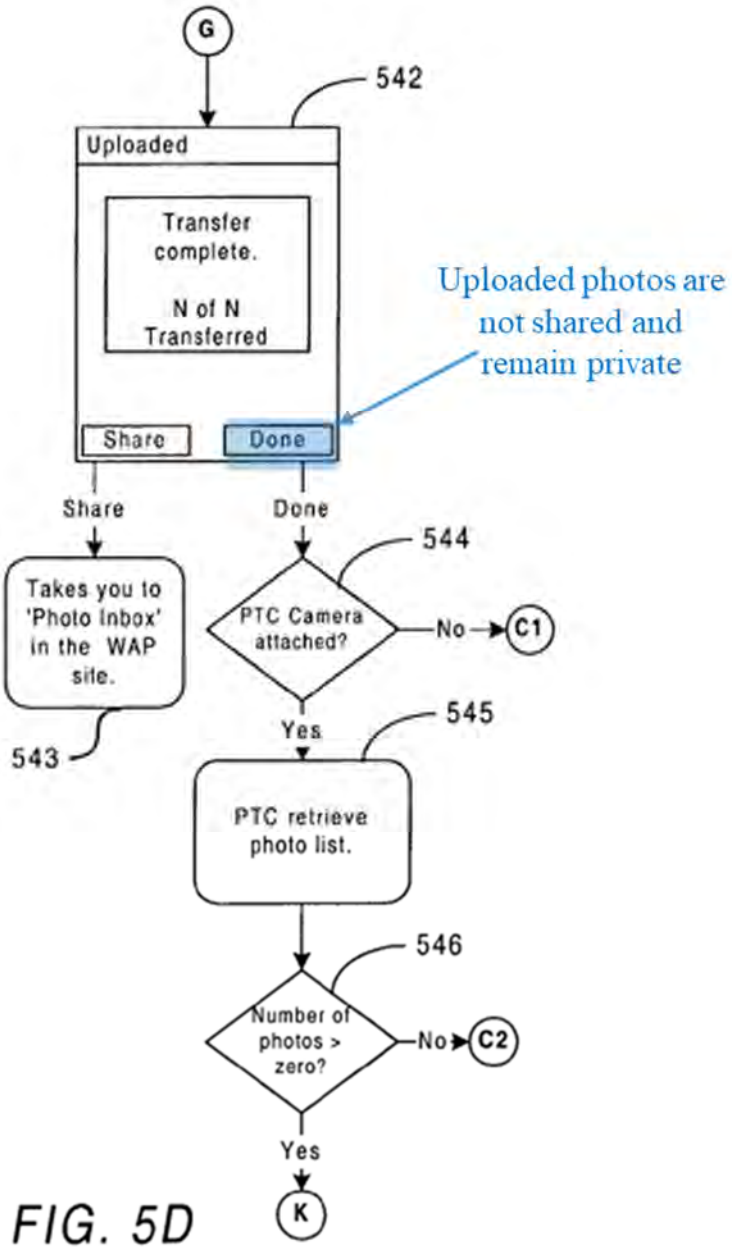


FIG. 5D

Kahn, FIG. 5D (annotated).

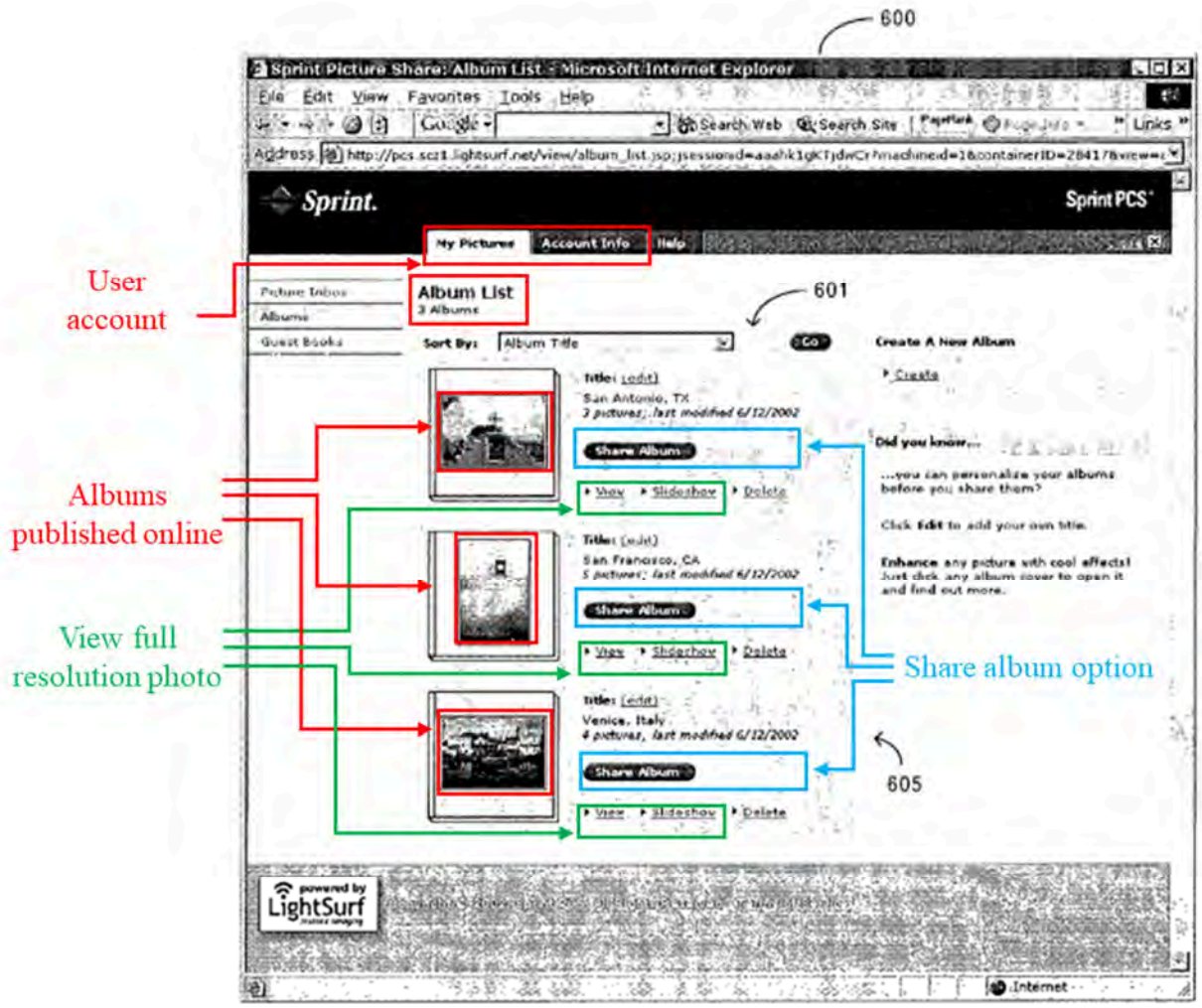


FIG. 6

Kahn, Fig. 6 (annotated).

Claim 2

[2] The short-range wireless enabled data capture device of claim 1, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

593. The Kahn-Bluetooth combination renders obvious [2]. Kahn-

Bluetooth teaches or suggests the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing. See Ground 2A, [1.3.1] and [1.3.2]

594. As mentioned above (See Ground 2A, [1.3.1]) Kahn teaches a "detachable connection" and in some instances, "cableless direct connection." Kahn, FIG. 3, [0045]. While Kahn does not expressly specify the type of communication for the wireless detachable connection between the camera and the cell phone, a POSITA would find it as an obvious choice to utilize Bluetooth, which was a commonly used technique to establish a "detachable connection", "cableless direct connection." Kahn, FIG. 3, [0045].

Claim 3

[3] The short-range wireless enabled data capture device of claim 1, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.

595. The Kahn-Bluetooth combination renders obvious [3]. In my opinion, Kahn-Bluetooth teaches or suggests the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data. For example, as discussed above (supra [1.5]), Kahn teaches capturing images (acquiring new-data), for example in step 701 of FIG. 7. During the image capturing process, Kahn also teaches acquiring associated new data that is also

digital data such as GPS location information and time stamp information., Kahn, [0058], [0008], [0098]. Moreover, a POSITA would have been motivated to, and it would have been obvious to, use the system for uploading text and video in addition to photographs, given that video cameras are, like Kahn's device, a camera, and video is a collection of images with one or more audio tracks. Because uploading need not be in real-time, the increased size of video files would not be prohibitive.

Claim 13

[13.P] A system, comprising:

596. To the extent the preamble is limiting, The Kahn-Bluetooth combination renders obvious [13.P]. Kahn-Bluetooth teaches or suggests a system. See Ground 2A, [1.P]. For example, Kahn teaches a "system 300 includes a camera device 310, a host device 320, and a GPS (Global Positioning System) module 325." Kahn, [0055]. Further, "the host device 320 communicates with an online Web-based image management server 330… accessible via the Internet." Kahn, [0056].

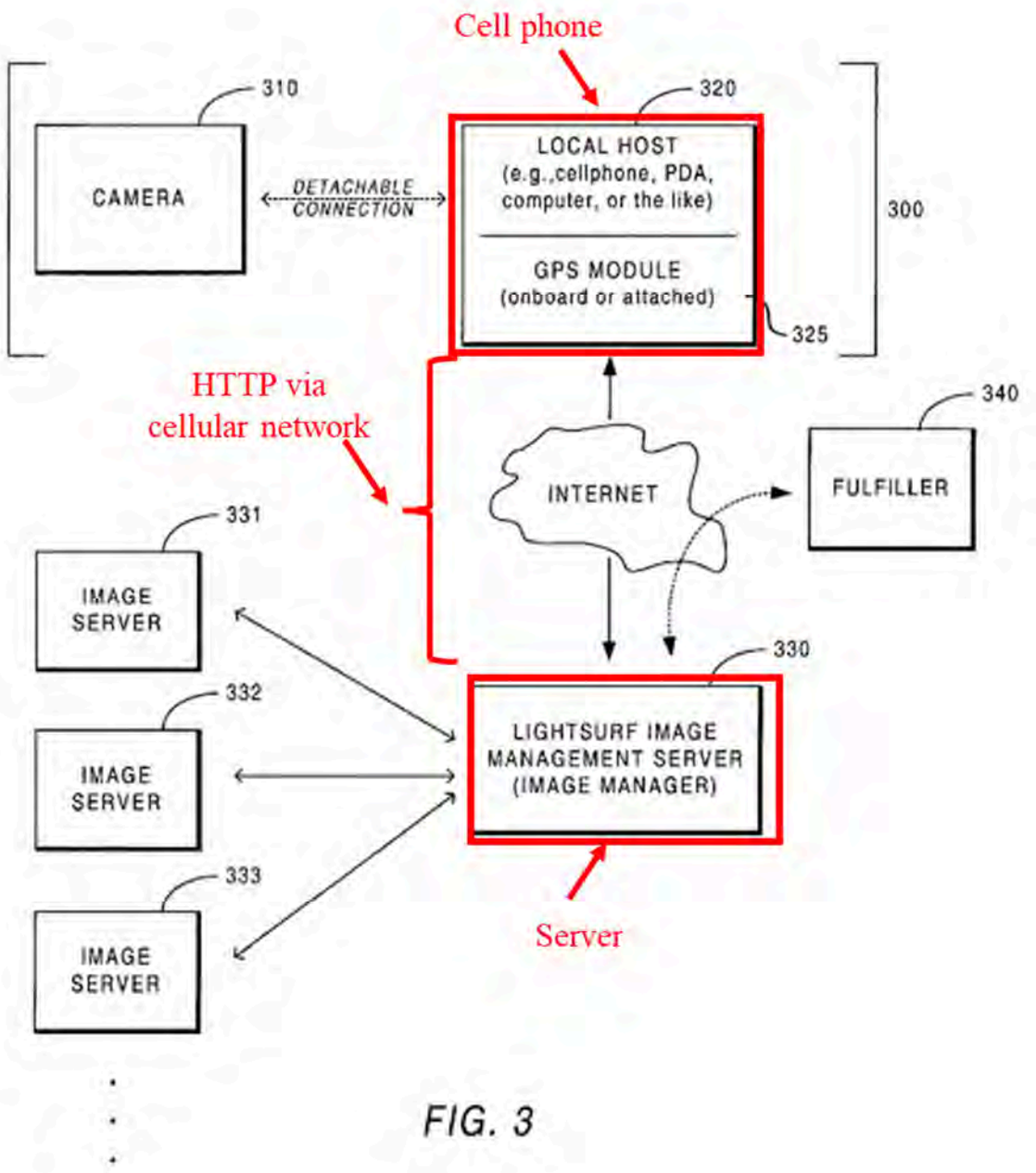


FIG. 3

Kahn, FIG. 3 (annotated).

597. In FIG. 4, Kahn "illustrates implementation of underlying functionality (i.e., processes) in the various modules of FIG. 3." Kahn, [0062]. The "system 400 includes the following functional modules: upload program 410,

location API 420, camera memory/API 430, server-side image manager application 440, image servers 450, and database (e.g., Oracle) 460 for storing metadata information." Kahn, [0062].

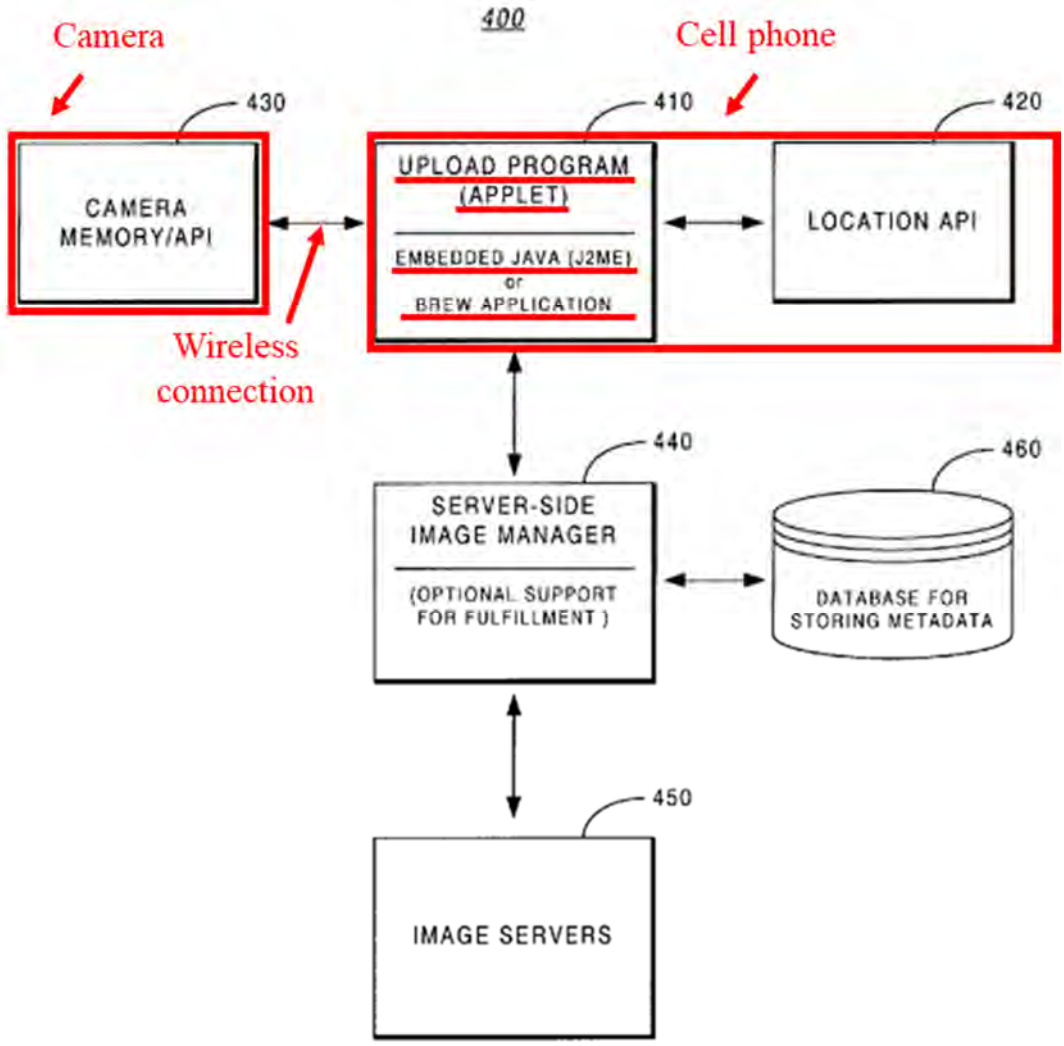


FIG. 4

Kahn, FIG. 4 (annotated).

[13.1] a short-range wireless enabled data capture device, comprising:

598. The Kahn-Bluetooth combination renders obvious [13.1]. Kahn-Bluetooth teaches or suggests a short-range wireless enabled data capture device. *See* Ground 2A, [1.P].

[13.2] a first memory device;

599. The Kahn-Bluetooth combination renders obvious [13.2]. Kahn-Bluetooth teaches or suggests a first memory device. See Ground 2A, [1.1].

[13.3] a first processor coupled to the first memory device;

600. The Kahn-Bluetooth combination renders obvious [13.3]. Kahn-Bluetooth teaches or suggests a first processor coupled to the first memory device. See Ground 2A, [1.2].

[13.4]-[13.6] a first short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone,
wherein establishing the short-range paired wireless connection comprises cryptographically authenticating identity of the short-range wireless enabled cellular phone, and
wherein establishing the short-range paired wireless connection further comprises the short-range wireless enabled data capture device using an association protocol;

601. The Kahn-Bluetooth combination renders obvious [13.4]-[13.6]. Kahn-Bluetooth teaches or suggests a first short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone, wherein establishing the short-range paired wireless

connection comprises cryptographically authenticating identity of the short-range wireless enabled cellular phone, and wherein establishing the short-range paired wireless connection further comprises the short-range wireless enabled data capture device using an association protocol. See Ground 2A, [1.3]-[1.5].

[13.7] a data capture circuitry;

602. The Kahn-Bluetooth combination renders obvious [13.7]. Kahn-Bluetooth teaches or suggests a data capture circuitry. See Ground 2A, [1.6].

[13.8] said first processor configured to acquire new-data using the data capture circuitry,
wherein the new-data is data acquired after the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone is established;

603. The Kahn-Bluetooth combination renders obvious [13.8]. Kahn-Bluetooth teaches or suggests said first processor configured to acquire new-data using the data capture circuitry, wherein the new-data is data acquired after the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone is established. See Ground 2A, [1.7]-[1.8].

[13.9] said first processor further configured to store the acquired new-data in the first memory device;

604. The Kahn-Bluetooth combination renders obvious [13.9]. Kahn-Bluetooth teaches or suggests said first processor further configured to store the acquired new-data in the first memory device. See Ground 2A, [1.9].

[13.10] said processor further configured to create a new-data object, wherein the new-data object comprises:

605. The Kahn-Bluetooth combination renders obvious [13.10]. Kahn-Bluetooth teaches or suggests said processor further configured to create a new-data object. See Ground 2A, [1.10].

[13.11] signal to notify, wherein the signal to notify corresponds to the acquiring of the new-data for transfer;

606. The Kahn-Bluetooth combination renders obvious [13.11]. Kahn-Bluetooth teaches or suggests signal to notify, wherein the signal to notify corresponds to the acquiring of the new-data for transfer. See Ground 2A, [1.11].

[13.12] the acquired new-data; and

607. The Kahn-Bluetooth combination renders obvious [13.12]. Kahn-Bluetooth teaches or suggests the acquired new-data. See Ground 2A, [1.12].

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

608. The Kahn-Bluetooth combination renders obvious [13.13]. Kahn-Bluetooth teaches or suggests associated new-data, wherein the associated new-data corresponds to data associated with the new-data. See Ground 2A, [1.13].

[13.14]-[13.15] said first processor further configured to receive a data transfer request from the short-range wireless enabled cellular phone, over the established short-range paired wireless connection,
wherein the data transfer request is for the acquired new-data that was acquired by the short-range wireless enabled data capture device before receiving the data transfer request; and

609. The Kahn-Bluetooth combination renders obvious [13.14]-[13.15].

Kahn-Bluetooth teaches or suggests said first processor further configured to receive a data transfer request from the short-range wireless enabled cellular phone, over the established short-range paired wireless connection, wherein the data transfer request is for the acquired new-data that was acquired by the short-range wireless enabled data capture device before receiving the data transfer request; and. See Ground 2A, [1.14], [1.7]-[1.8]. Kahn teaches a camera (first processor) configured to receive a data transfer request from a cell phone. For example, Kahn teaches "the applet displays UI dialog 550 (FIG. 5E), which allows access to individual images on the camera. Here, the user is given a variety of options, as indicated by dialog 551: upload this photo, delete this photo, upload all photos, delete all photos, or exit." TTI-1017, [0079]. Upon selecting the "upload images" options, a POSITA would have understood that the applet is sending a transfer request to the camera to upload photos to the server via cell phone.

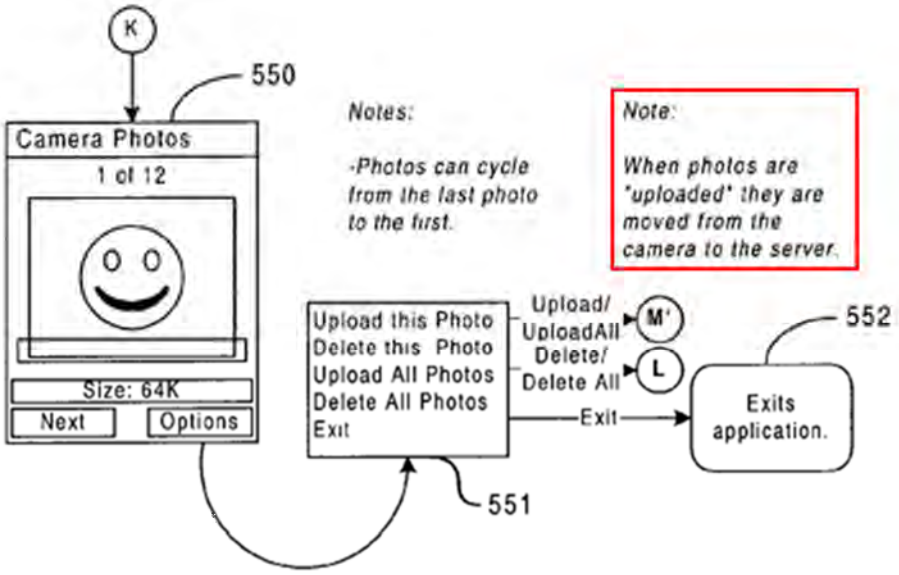


FIG. 5E

TTI-1017, FIG. 5E (partial) (annotated).

[13.16] said first processor configured to transfer the new-data object to the short-range wireless enabled cellular phone over the established short-range paired wireless connection;

610. The Kahn-Bluetooth combination renders obvious [13.16]. Kahn-Bluetooth teaches or suggests said first processor configured to transfer the new-data object to the short-range wireless enabled cellular phone over the established short-range paired wireless connection. See Ground 2A, [1.14].

[13.17] a mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that, when executed by a second processor of the short-range wireless enabled cellular phone controls the second processor to:

611. The Kahn-Bluetooth combination renders obvious [13.17]. Kahn-Bluetooth teaches or suggests a mobile client application for the short-range

wireless enabled cellular phone comprising executable instructions executed by a second processor of the short-range wireless enabled cellular phone that controls the second processor. For example, Kahn has a mobile client application. See Ground 2A, [1.16]. Kahn teaches "the client-side applet program, which may be embodied as an embedded J2ME applet in the local host" for example a cell phone. Kahn, [0071], [0055]. Kahn teaches that "a client-side embedded applet (i.e., a small footprint application) [that] executes method steps and displays exemplary user interface (UI) dialogs/menus for supporting fulfillment." Kahn, [0071], FIGs. 5A-5F.

612. A POSITA would have recognized that the cell phone would have included a processor for processing executable instruction of the applet. A POSITA would have recognized that a cell phone would have implemented at least one processor to execute "computer-executable instructions, for directing operation of a device under processor control." Kahn, [0052].

[13.18]-[13.19] receive a request through a graphical user interface (GUI) of the cryptographically authenticated short-range wireless enabled cellular phone for new-data and send a data transfer request to the short-range wireless enabled data capture device, over the established short-range paired wireless connection,
wherein the data transfer request is for the acquired new-data that was acquired by the short-range wireless enabled data capture device before receiving the data transfer request;

613. The Kahn-Bluetooth combination renders obvious [13.18]-[13.19]. Kahn-Bluetooth teaches or suggests receive a request through a graphical user

interface (GUI) of the cryptographically authenticated short-range wireless enabled cellular phone for new-data and send a data transfer request to the short-range wireless enabled data capture device, over the established short-range paired wireless connection, wherein the data transfer request is for the acquired new-data that was acquired by the short-range wireless enabled data capture device before receiving the data transfer request. See Ground 2A, [1.4], [1.8], [1.16.1]. For example, Kahn illustrates, in "FIGS. 5A-F illustrate execution of a client-side embedded applet (i.e., a small footprint application) that executes method steps and displays exemplary user interface (UI) dialogs/menus for supporting fulfillment." Kahn, [0025], [0070]-[0071], FIGs. 5A-F.

[13.20] receive the new-data object from the short-range wireless enabled data capture device, over the established short-range paired wireless connection;

614. The Kahn-Bluetooth combination renders obvious [13.20]. Kahn-Bluetooth teaches or suggests receive the new-data object from the short-range wireless enabled data capture device, over the established short-range paired wireless connection. See Ground 2A, [1.10], [1.14].

[13.21] store the new-data received over the established short-range paired wireless connection, in a second memory device of the short-range wireless enabled cellular phone; and

615. The Kahn-Bluetooth combination renders obvious [13.21]. Kahn-Bluetooth teaches or suggests store the new-data received over the established short-range paired wireless connection, in a second memory device of the short-

range wireless enabled cellular phone. See Ground 2A, [1.16.1], [1.16.2].

[13.22]-[13.23] use HTTP to upload 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.

616. The Kahn-Bluetooth combination renders obvious [13.22]-[13.23]. Kahn-Bluetooth teaches or suggests use HTTP to upload 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. See Ground 2A, [1.17]-[1.18].

Claim 14

[14] The system of claim 13, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

617. The Kahn-Bluetooth combination renders obvious [14]. Kahn-Bluetooth teaches or suggests the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing. See Ground 2A, [2].

Claim 15

[15] The system of claim 13, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.

618. The Kahn-Bluetooth combination renders obvious [15]. Kahn-Bluetooth teaches or suggests 15. The system of claim 13, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data. See Ground 2A, [3].

Claim 9

[9.P] A short-range wireless enabled cellular phone, comprising:

619. To the extent the preamble is limiting, The Kahn-Bluetooth combination renders obvious [9.P]. Kahn-Bluetooth teaches or suggests a short-range wireless enabled cellular phone. For example, Kahn teaches a "system 300 includes a camera device 310, a host device 320, and a GPS (Global Positioning System) module 325." Kahn, [0055]. Further, the "host device 320 may comprise a cellular phone, a PDA (personal data assistant) with wireless connectivity, or the like.", Kahn, [0056]. Kahn also teaches that "a host device 320 that can be a mobile phone, Kahn, [0045] ("the digital camera 100 would occasionally be connected to a local host device, such as a cellular phone"). Kajn teached that "the host device 320 communicates with an online Web-based image management server 330… accessible via the Internet." Kahn, [0056].

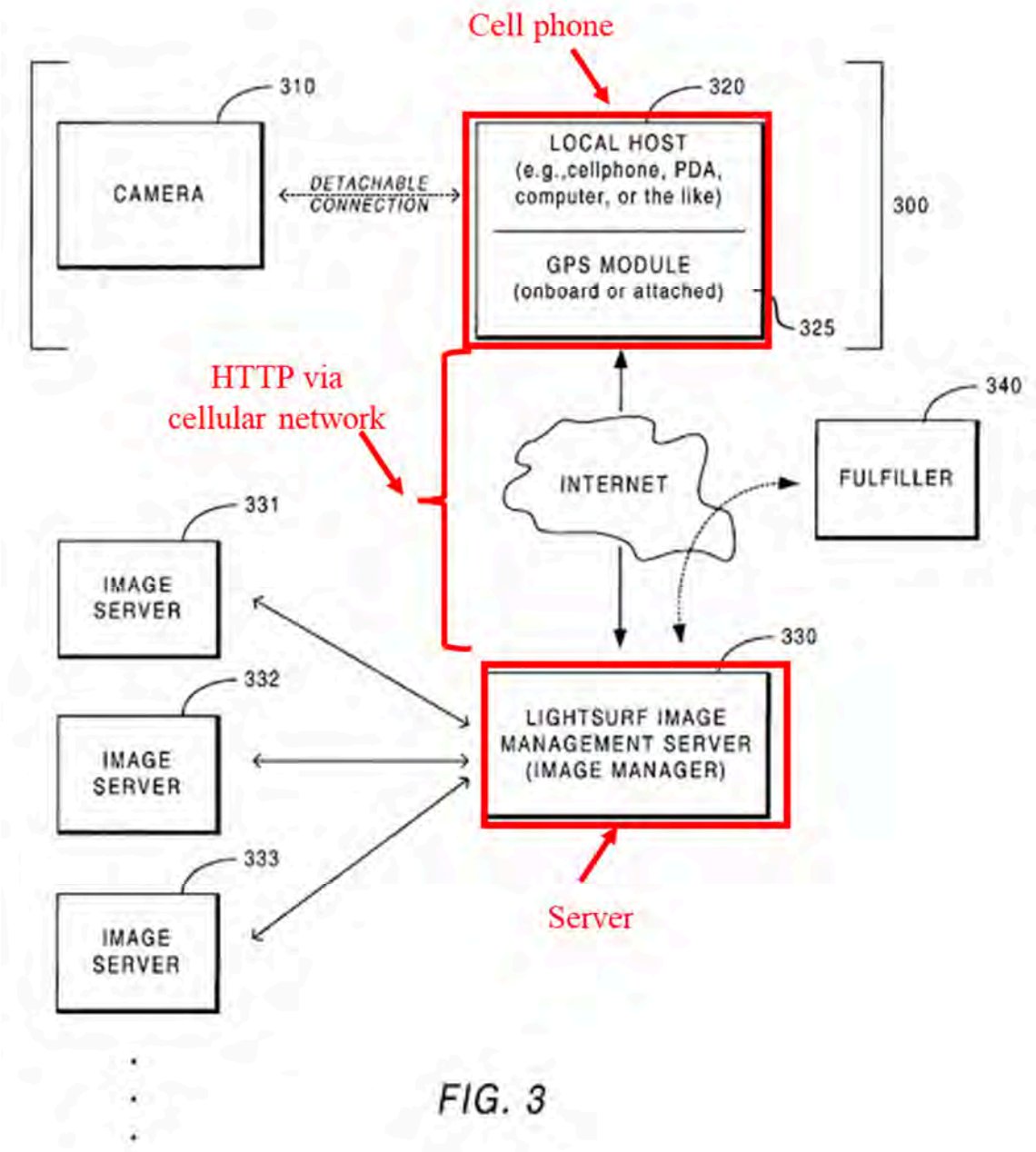


FIG. 3

Kahn, FIG. 3 (annotated).

620. In FIG. 4, Kahn "illustrates implementation of underlying functionality (i.e., processes) in the various modules of FIG. 3." Kahn, [0062]. The "system 400 includes the following functional modules: upload program 410,

location API 420, camera memory/API 430, server-side image manager application 440, image servers 450, and database (e.g., Oracle) 460 for storing metadata information." Kahn, [0062].

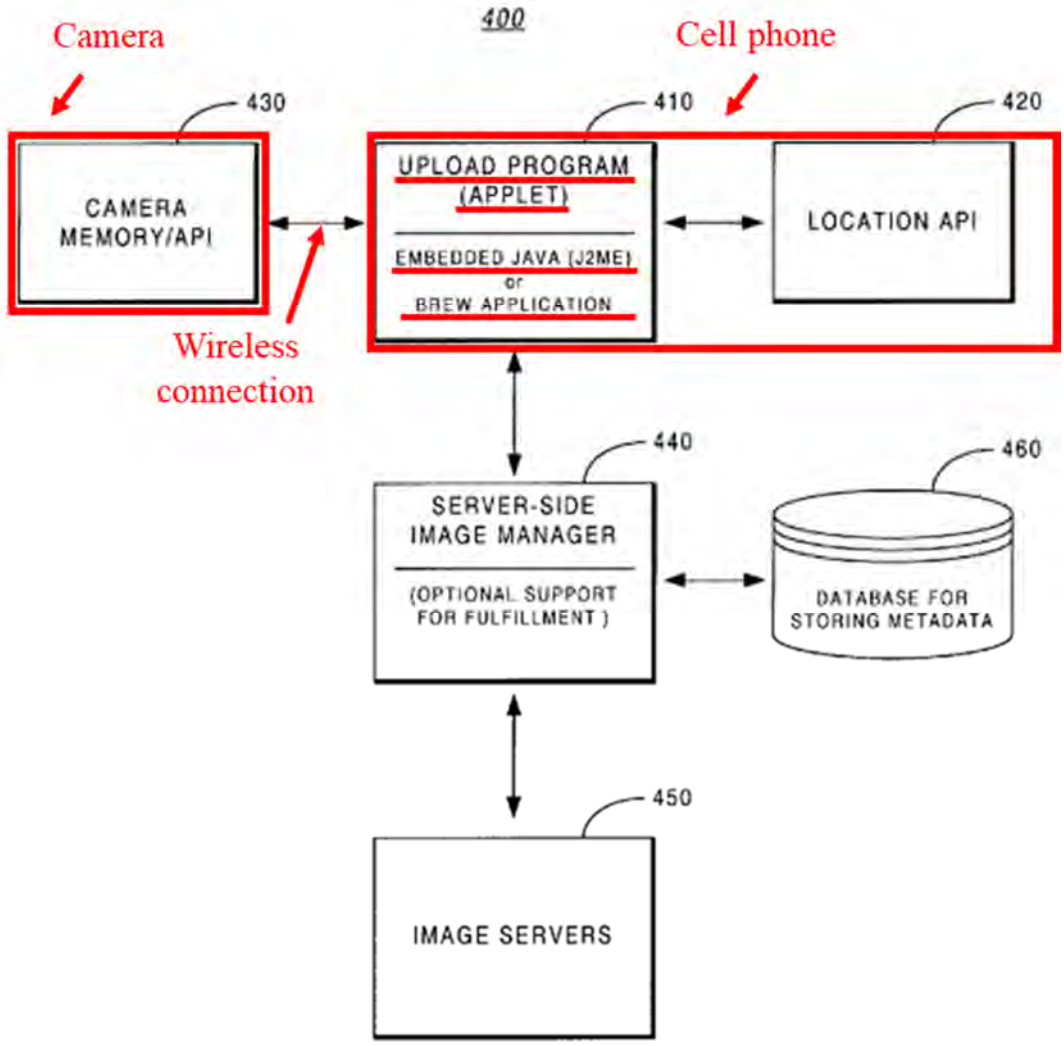


FIG. 4

Kahn, FIG. 4 (annotated).

[9.1] a memory device;

621. The Kahn-Bluetooth combination renders obvious [9.1]. Kahn-Bluetooth teaches or suggests a memory device. See Ground 2A, [1.13.2].

[9.2] a processor coupled to said memory device;

622. The Kahn-Bluetooth combination renders obvious [9.2]. Kahn-Bluetooth teaches or suggests a processor coupled to said memory device. See Ground 2A, [9.P] and [9.1]. Kahn-Bluetooth teaches or suggests a mobile client application for the short-range wireless enabled cellular phone comprising executable instructions executed by the processor. For example, Kahn had a mobile client application. See Ground 2A, [1.13.1], [1.13.2]. Kahn teaches "the client-side applet program, which may be embodied as an embedded J2ME applet in the local host" for example a cell phone. Kahn, [0071], [0055]. Kahn teaches that "a client-side embedded applet (i.e., a small footprint application) [that] executes method steps and displays exemplary user interface (UI) dialogs/menus for supporting fulfillment." Kahn, [0071].

623. A POSITA would have recognized that the cell phone would have included a processor for processing executable instruction of the applet and mobile phones had processors to perform operations.

624. Further, during uploading process, Kahn teaches "transfer[ing] of the images from the camera to the host (e.g., cell phone), for uploading to a destination image server." Kahn, [0063]. Kahn also teaches that once the photo is uploaded,

the applet deletes the photo from the cell phone's memory. Kahn, [0085] ("step 540, where the photo is deleted (from local storage)."), FIG. 5D (figure element 540). Thus, a POSITA would have understood that in order to delete the photo from the cell phone's memory, the photo would have been stored by the processor in the first place. Thus, a POSITA would have understood that the cell phone's processor is coupled to a memory device.

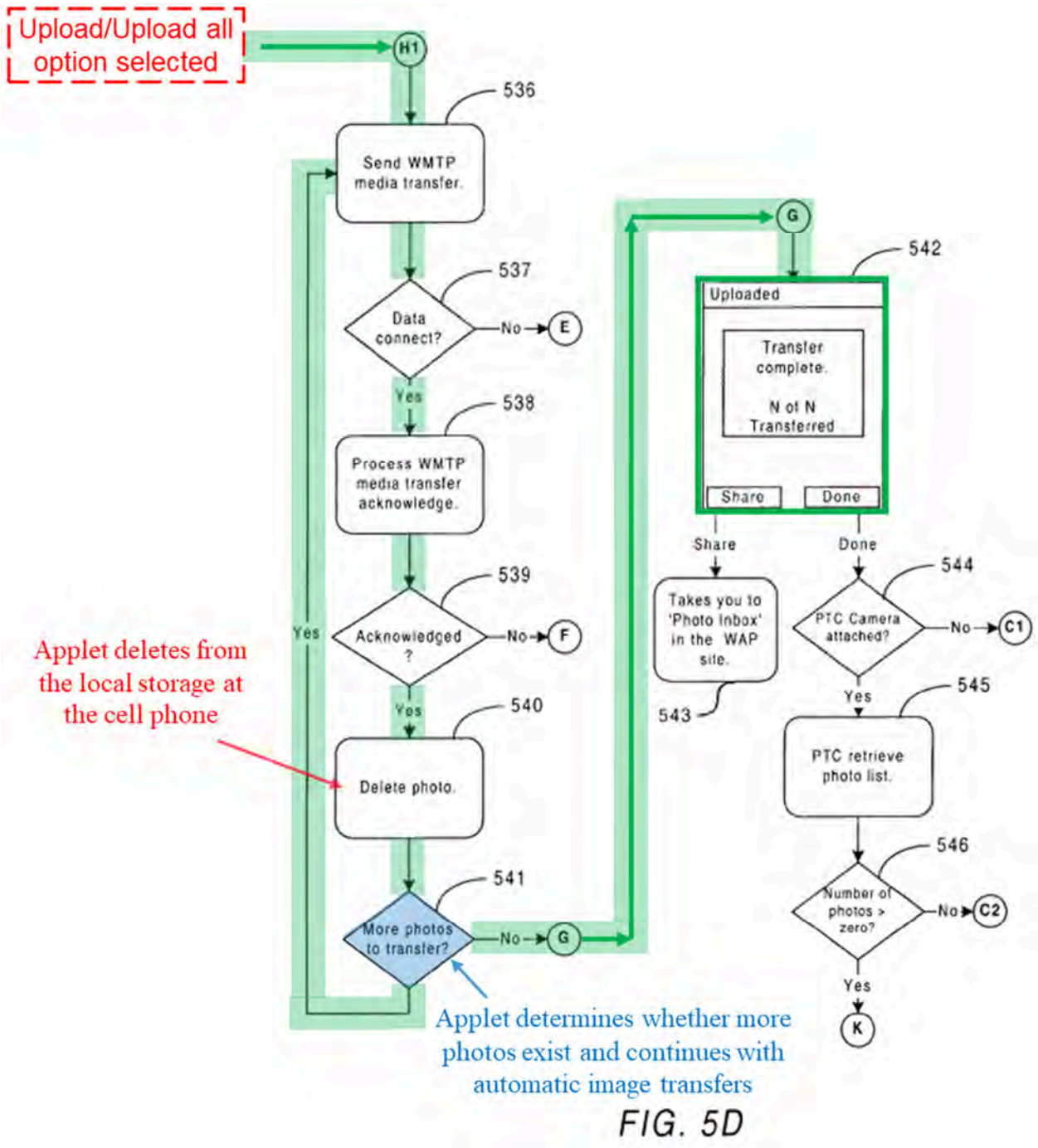


FIG. 5D

Kahn, FIG. 5D (annotated).

[9.3] a cellular network communication device configured to connect to internet via a cellular data network;

625. The Kahn-Bluetooth combination renders obvious [9.3]. Kahn-

Bluetooth teaches or suggests a cellular network communication device configured to connect to internet via a cellular data network. For example, Kahn teaches "the host device 320 communicates with an online Web-based image management server 330… accessible via the Internet." Kahn, [0056]. Kahn also teaches that the cell phone is connect to the internet using cellular network. Kahn, [0008], [0010].

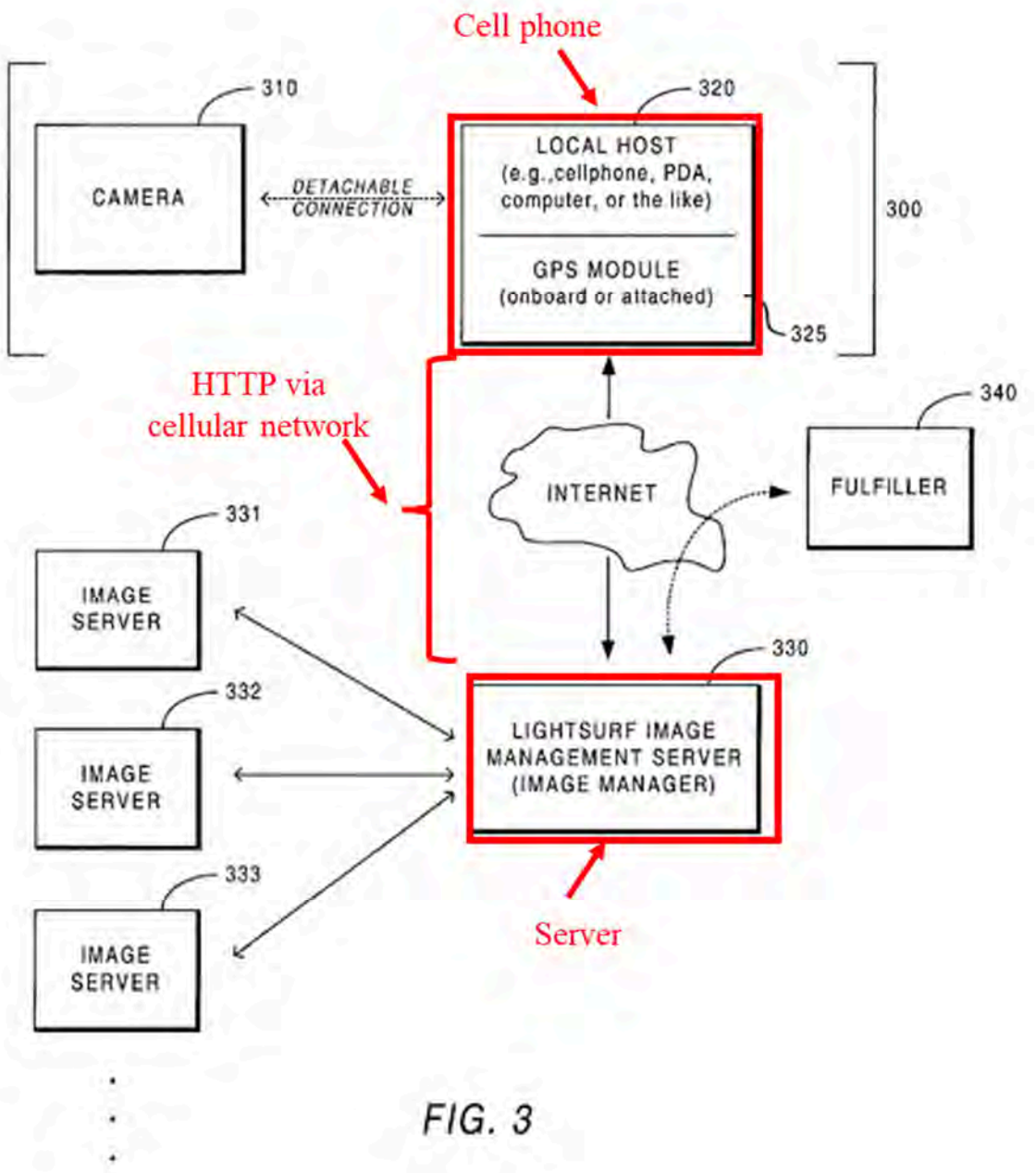


FIG. 3

Kahn, FIG. 3 (annotated).

[9.4]-[9.6] a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled cellular phone and a short-range wireless enabled data capture device,
wherein the short-range wireless enabled data capture device is configured to cryptographically authenticate identity of the short-range wireless enabled

cellular phone when establishing the short-range paired wireless connection, and
wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled mobile device using an association protocol;

626. The Kahn-Bluetooth combination renders obvious [9.4]-[9.6]. Kahn-Bluetooth teaches or suggests a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled cellular phone and a short-range wireless enabled data capture device, wherein the short-range wireless enabled data capture device is configured to cryptographically authenticate identity of the short-range wireless enabled cellular phone when establishing the short-range paired wireless connection, and wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled mobile device using an association protocol. See Ground 2A, [1.3]-[1.5].

[9.7] a mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that, when executed by the processor controls the processor to:

627. The Kahn-Bluetooth combination renders obvious [9.7]. Kahn-Bluetooth teaches or suggests a mobile client application for the short-range wireless enabled cellular phone comprising executable instructions executed by the processor. For example, Kahn had a mobile client application. See Ground 2A, [1.13]. Kahn teaches "the client-side applet program, which may be embodied as an embedded J2ME applet in the local host" for example a cell phone. Kahn,

[0071], [0055]. Kahn teaches that "a client-side embedded applet (i.e., a small footprint application) [that] executes method steps and displays exemplary user interface (UI) dialogs/menus for supporting fulfillment." Kahn, [0071].

628. A POSITA would have recognized that the cell phone would have included a processor for processing executable instruction of the applet. A POSITA would have recognized that a cell phone would have implemented at least one processor to execute "computer-executable instructions, for directing operation of a device under processor control." Kahn, [0052]. See also, Ground 2A, [1.16]; Ground 2A, [9.2].

[9.8]-[9.9] receive a new-data object from the short-range wireless enabled data capture device over the established short-range paired wireless connection, wherein the new-data object comprises:

629. The Kahn-Bluetooth combination renders obvious [9.8]. Kahn-Bluetooth teaches or suggests receiving a new-data object from the short-range wireless enabled data capture device over the established short-range paired wireless connection. See Ground 2A, [1.14]. For example, Kahn teaches that the new data object goes from the camera, to the cell phone, and then to the server as shown in FIG. 5D, Kahn illustrates automatic "transfer of the images from the camera to the host (e.g., cell phone), for uploading to a destination image server.", Kahn, [0063].

[9.10]-[9.12] signal to notify and acquired new-data, wherein the acquired new-data is data acquired by the short-range wireless

enabled data capture device after the short-range paired wireless connection is established between the short-range wireless enabled cellular phone and the short-range wireless enabled data capture device, and
wherein the signal to notify corresponds to the acquiring of the new-data for transfer; and

630. The Kahn-Bluetooth combination renders obvious [9.10]-[9.12]. Kahn-Bluetooth teaches or suggests signal to notify and acquired new-data, wherein the acquired new-data is data acquired by the short-range wireless enabled data capture device after the short-range paired wireless connection is established between the short-range wireless enabled cellular phone and the short-range wireless enabled data capture device, and wherein the signal to notify corresponds to the acquiring of the new-data for transfer. See Ground 2A, [1.11], and [1.12].

[9.13] associated new-data, wherein the associated new-data corresponds to data associated with the new-data;

631. The Kahn-Bluetooth combination renders obvious [9.13]. Kahn-Bluetooth teaches or suggests associated new-data, wherein the associated new-data corresponds to data associated with the new-data. See Ground 2A, [1.13].

[9.14] listen and process the signal to notify;

632. The Kahn-Bluetooth combination renders obvious [9.14]. Kahn-Bluetooth teaches or suggests listen and process the signal to notify. See Ground 2A, [1.15] and [1.16.1].

[9.15] store the received new-data in the memory device; and

633. The Kahn-Bluetooth combination renders obvious [9.15]. Kahn-

Bluetooth teaches or suggests store the received new-data in the memory device. See Ground 2A, [1.16.2].

[9.16]-[9.17] 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.

634. The Kahn-Bluetooth combination renders obvious [9.16]-[9.17]. Kahn-Bluetooth teaches or suggests 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. See Ground 2A, [1.17] and [1.18].

Claim 10

[10] The short-range wireless enabled cellular phone of claim 9, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

635. The Kahn-Bluetooth combination renders obvious [10]. Kahn-Bluetooth teaches or suggests the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing. See Ground 2A, [2].

Claim 11

[11] The short-range wireless enabled cellular phone of claim 9, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.

636. The Kahn-Bluetooth combination renders obvious [11]. Kahn-Bluetooth teaches or suggests the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data. See Ground 2A, [3].

Claim 12

[12] The short-range wireless enabled cellular phone of claim 9, wherein a graphical user interface (GUI) is provided in the cryptographically authenticated short-range wireless enabled cellular phone, and wherein the graphical user interface (GUI) is for the received new-data.

637. The Kahn-Bluetooth combination renders obvious [12]. Kahn-Bluetooth teaches or suggests a graphical user interface (GUI) is provided in the cryptographically authenticated short-range wireless enabled cellular phone, and wherein the graphical user interface (GUI) is for the received new-data. See Ground 2A, [8]. For example, Kahn illustrates, in "FIGS. 5A-F illustrate execution of a client-side embedded applet (i.e., a small footprint application) that executes method steps and displays exemplary user interface (UI) dialogs/menus for supporting fulfillment." Kahn, [0025], [0070]-[0071], FIGs. 5A-F.

Claim 4

[4.P] A system, comprising:

638. To the extent the preamble is limiting, The Kahn-Bluetooth combination renders obvious [4.P]. Kahn-Bluetooth teaches or suggests a system. See Ground 2A, [13.P]. For example, Kahn teaches a "system 300 includes a camera device 310, a host device 320, and a GPS (Global Positioning System) module 325." Kahn, [0055]. Further, "the host device 320 communicates with an online Web-based image management server 330… accessible via the Internet." Kahn, [0056].

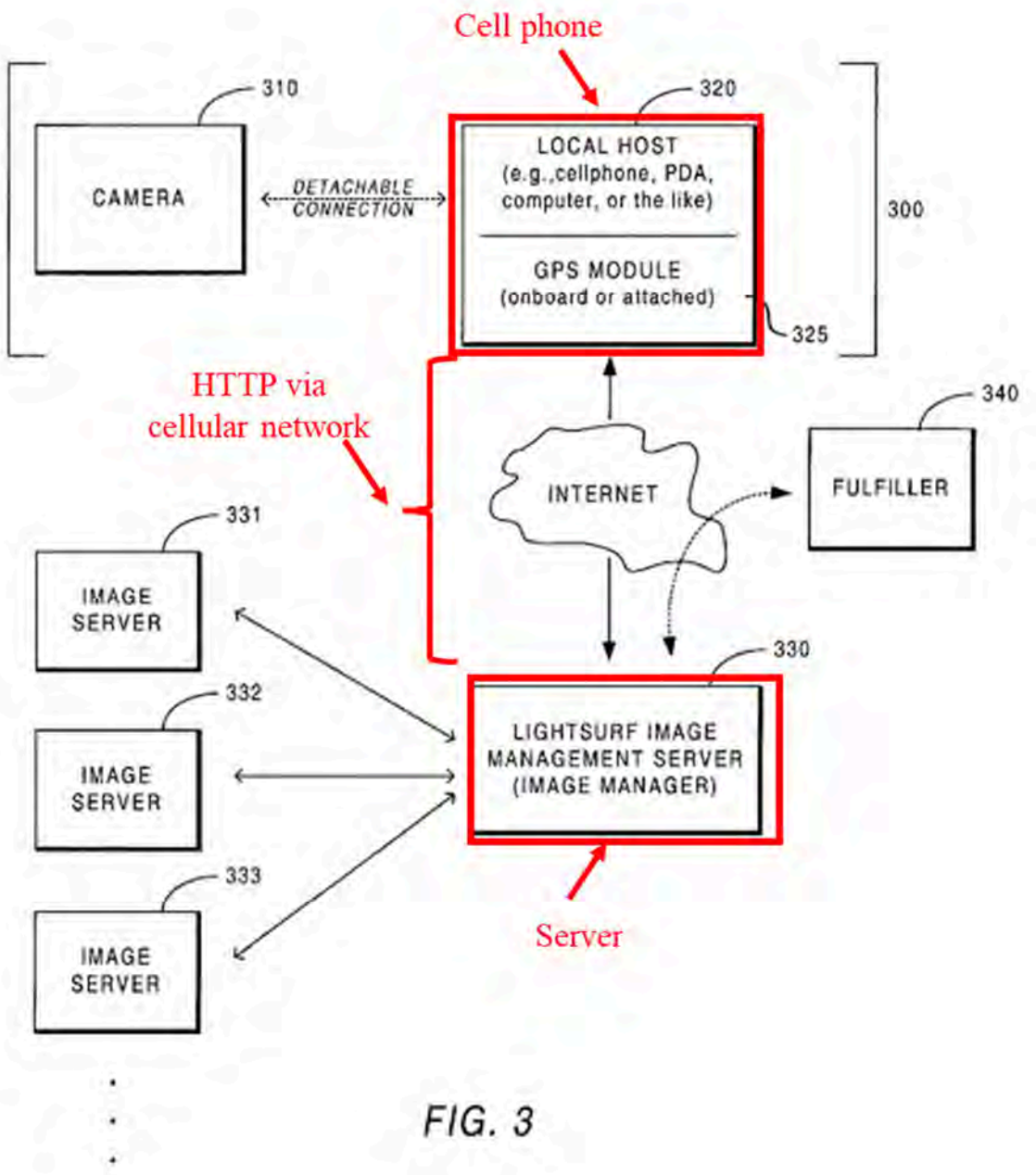


FIG. 3

Kahn, FIG. 3 (annotated).

639. In FIG. 4, Kahn "illustrates implementation of underlying functionality (i.e., processes) in the various modules of FIG. 3." Kahn, [0062]. The "system 400 includes the following functional modules: upload program 410,

location API 420, camera memory/API 430, server-side image manager application 440, image servers 450, and database (e.g., Oracle) 460 for storing metadata information." Kahn, [0062].

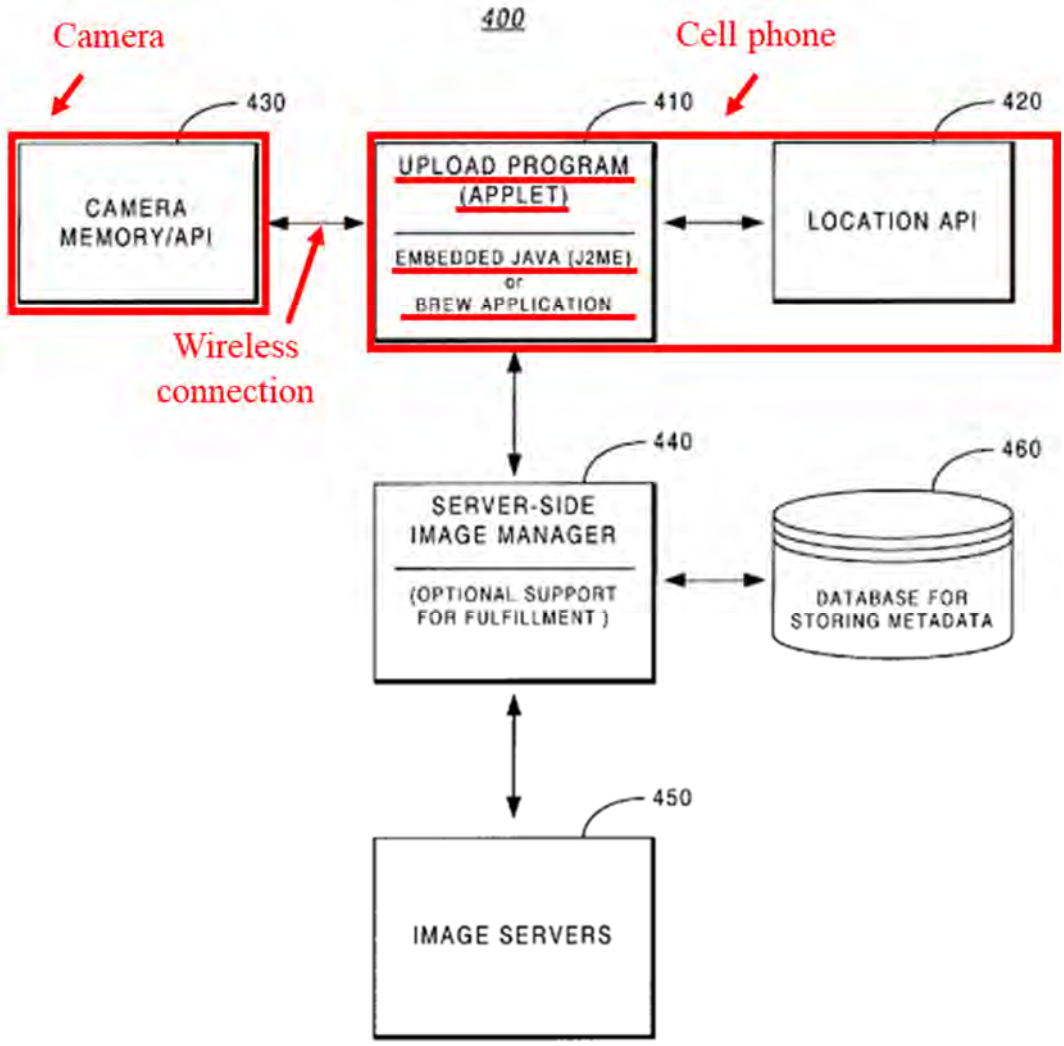


FIG. 4

Kahn, FIG. 4 (annotated).

[4.1] a data capture device, comprising:

640. The Kahn-Bluetooth combination renders obvious [4.1]. Kahn-Bluetooth teaches or suggests a data capture device. See Ground 2A, [13.1].

[4.2] a first memory device;

641. The Kahn-Bluetooth combination renders obvious [4.2]. Kahn-Bluetooth teaches or suggests a first memory device. See Ground 2A, [13.2].

[4.3] a first processor coupled to the first memory device;

642. The Kahn-Bluetooth combination renders obvious [4.3]. Kahn-Bluetooth teaches or suggests a first processor coupled to the first memory device. See Ground 2A, [13.3].

[4.4]-[4.6] a first short-range wireless communication device configured to establish a short-range paired wireless connection with an internet connected cellular phone,
wherein establishing the short-range paired wireless connection comprises, the data capture device cryptographically authenticating identity of the cellular phone, and wherein establishing the short-range paired wireless connection further comprises the data capture device using an association protocol;

643. The Kahn-Bluetooth combination renders obvious [4.4]-[4.6]. Kahn-Bluetooth teaches or suggests a first short-range wireless communication device configured to establish a short-range paired wireless connection with an internet connected cellular phone, wherein establishing the short-range paired wireless connection comprises, the data capture device cryptographically authenticating identity of the cellular phone, and wherein establishing the short-range paired wireless connection further comprises the data capture device using an association

protocol. See Ground 2A, [13.4]-[13.6], [1.3]-[1.5].

[4.7] a data capture circuitry;

644. The Kahn-Bluetooth combination renders obvious [4.7]. Kahn-Bluetooth teaches or suggests a data capture circuitry. See Ground 2A, [13.7], [1.6].

[4.8]-[4.9] said first processor configured to acquire new-data in the data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection with the cellular phone;

645. The Kahn-Bluetooth combination renders obvious [4.8]-[4.9]. Kahn-Bluetooth teaches or suggests said first processor configured to acquire new-data in the data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection with the cellular phone. See Ground 2A, [13.8], [1.7]-[1.8].

[4.10] said first processor further configured to store the new-data in the first memory device;

646. The Kahn-Bluetooth combination renders obvious [4.10]. Kahn-Bluetooth teaches or suggests said first processor further configured to store the new-data in the first memory device. See Ground 2A, [13.9], [1.9].

[4.11] said first processor further configured to create a new-data object, wherein the new-data object comprises:

647. The Kahn-Bluetooth combination renders obvious [4.11]. Kahn-Bluetooth teaches or suggests said first processor further configured to create a

new-data object. See Ground 2A, [13.10], [1.10].

[4.12] signal to notify, wherein the signal to notify corresponds to the acquiring of the new-data for transfer to the cryptographically authenticated cellular phone;

648. The Kahn-Bluetooth combination renders obvious [4.12]. Kahn-Bluetooth teaches or suggests signal to notify, wherein the signal to notify corresponds to the acquiring of the new-data for transfer to the cryptographically authenticated cellular phone. See Ground 2A, [13.11], [1.11].

[4.13] the acquired new-data; and

649. The Kahn-Bluetooth combination renders obvious [4.13]. Kahn-Bluetooth teaches or suggests the acquired new-data; and. See Ground 2A, [13.12], [1.12].

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

650. The Kahn-Bluetooth combination renders obvious [4.14]. Kahn-Bluetooth teaches or suggests associated new-data, wherein the associated new-data corresponds to data associated with the new-data. See Ground 2A, [13.13], [1.13].

[4.15] said first processor further configured to transfer automatically the new-data object to the cryptographically authenticated cellular phone, over the established short-range paired wireless connection;

651. The Kahn-Bluetooth combination renders obvious [4.15]. Kahn-Bluetooth teaches or suggests said first processor further configured to transfer

automatically the new-data object to the cryptographically authenticated cellular phone, over the established short-range paired wireless connection. See Ground 2A, [13.16], [1.14].

[4.16] said cellular phone, comprising:

652. The Kahn-Bluetooth combination renders obvious [4.16]. Kahn-Bluetooth teaches or suggests said cellular phone. See Ground 2A, [9.P].

[4.17] a second memory device;

653. The Kahn-Bluetooth combination renders obvious [4.17]. Kahn-Bluetooth teaches or suggests a second memory device. See Ground 2A, [9.1].

[4.18] a second processor coupled to said second memory device;

654. The Kahn-Bluetooth combination renders obvious [4.18]. Kahn-Bluetooth teaches or suggests a second processor coupled to said second memory device. See Ground 2A, [9.2].

[4.19] a cellular network communication device configured to connect to the internet via the cellular data network;

655. The Kahn-Bluetooth combination renders obvious [4.19]. Kahn-Bluetooth teaches or suggests a cellular network communication device configured to connect to the internet via the cellular data network. See Ground 2A, [9.3].

[4.20] a second short-range wireless communication device configured to establish the short-range paired wireless connection between the cellular phone and the data capture device;

656. The Kahn-Bluetooth combination renders obvious [4.20]. Kahn-

Bluetooth teaches or suggests a second short-range wireless communication device configured to establish the short-range paired wireless connection between the cellular phone and the data capture device. See Ground 2A [4.4]-[4.6] and [9.4]-[9.6]. A POSITA would find it obvious that by connecting a camera to a cell phone via Bluetooth that the connected cell phone would also feature a comparable communication device to establish connection with the camera.

[4.21] a mobile client application for the cellular phone comprising executable instructions that, when executed by the second processor controls the second processor to:

657. The Kahn-Bluetooth combination renders obvious [4.21]. Kahn-Bluetooth teaches or suggests a mobile client application for the cellular phone comprising executable instructions executed by the second processor. See Ground 2A, [9.7].

[4.22] listen for the signal to notify;

658. The Kahn-Bluetooth combination renders obvious [4.22]. Kahn-Bluetooth teaches or suggests listen for the signal to notify. See Ground 2A, [9.14].

[4.23] receive the new-data object from the data capture device;

659. The Kahn-Bluetooth combination renders obvious [4.23]. Kahn-Bluetooth teaches or suggests receive the new-data object from the data capture device. See Ground 2A, [9.8]-[9.9].

[4.24] store the received new-data in the second memory device; and

660. The Kahn-Bluetooth combination renders obvious [4.24]. Kahn-Bluetooth teaches or suggests store the received new-data in the second memory device. See Ground 2A, [9.15].

[4.25]-[4.26] 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.

661. The Kahn-Bluetooth combination renders obvious [4.25]-[4.26]. Kahn-Bluetooth teaches or suggests 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. See Ground 2A, [9.16]-[9.17].

Claim 5

[5] The system of claim 4, wherein establishing the short-range paired wireless connection comprises the data capture device using an association protocol.

662. The Kahn-Bluetooth combination renders obvious [5]. Kahn-Bluetooth teaches or suggests establishing the short-range paired wireless connection comprises the data capture device using an association protocol. See Ground 2A, [1.3].

Claim 6

[6] The system of claim 4, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

663. The Kahn-Bluetooth combination renders obvious [6]. Kahn-Bluetooth teaches or suggests the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing. See Ground 2A, [2].

Claim 7

[7] The system of claim 4, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.

664. The Kahn-Bluetooth combination renders obvious [7]. Kahn-Bluetooth teaches or suggests the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data. See Ground 2A, [3].

Claim 8

[8] The system of claim 4, wherein a graphical user interface (GUI) is provided in the cryptographically authenticated cellular phone, and wherein the graphical user interface (GUI) is for the received new-data.

665. The Kahn-Bluetooth combination renders obvious [8]. Kahn-Bluetooth teaches or suggests a graphical user interface (GUI) is provided in the cryptographically authenticated cellular phone, and wherein the graphical user

interface (GUI) is for the received new-data. For example, Kahn illustrates, in "FIGS. 5A-F illustrate execution of a client-side embedded applet (i.e., a small footprint application) that executes method steps and displays exemplary user interface (UI) dialogs/menus for supporting fulfillment." Kahn, [0025], [0070]-[0071], FIGs. 5A-F. See Ground 2A, [1.7]-[1.14].

C. Ground 2B: Kahn in view of Feinberg and Bluetooth renders claims 1-15 obvious

1. Motivation to Combine Kahn and Feinberg

666. In the proposed combination, as described by Kahn, the system automatically transmits a new data object that includes a new data and associated new data. Thumbnails are created by the camera and transmitted to the mobile phone for previewing new images captured by the camera. In the combination, based on Feinberg, thumbnails of the new images are embedded into the full resolution image file header as a signal to notify, in a manner suggested by Feinberg, so that the new data object automatically transmitted from the camera to the mobile phone also includes the thumbnails. A POSITA at the time of the invention would have been motivated to combine the teachings of Kahn and Feinberg, thus rendering the subject matter of the '766 patent challenged claims (claims 1-15) obvious.

667. First, both Kahn and Feinberg are analogous art to the claimed invention. Both references are from the same field of endeavor as the claimed invention: wireless image transfer from one electronic device to another. Kahn is directed to wirelessly transferring image files from a mobile device to a publishing website over the Internet with an HTTP action setting. *See, e.g.,* Kahn, [0056], [0077] (describing the action setting of creating a new album on the server for uploading the images). Likewise, Feinberg teaches "digital cameras having wireless network connectivity … with wireless networks (usually such networks as are compliant with the IEEE 802.11 a/b/g standards) to transfer image data from the media card to a personal computer or printer." Feinberg, [0005]. Feinberg also teaches "images are uploaded from a camera to an Internet-based computer/storage resource, … using a … mobile phone." Feinberg, [0049]. Both Kahn and Feinberg concern the wireless transmission of images between a camera, a mobile phone, and a remote server.

668. Kahn and Feinberg are also pertinent to the problem of the '766 patent: transmission of image data by a cellular phone that was captured by a digital camera. ['766 patent], Background. Kahn addresses the problem through efficient publishing of image data from a cellular phone to a website using HTTP. *See, e.g*., Kahn, [0056], [0063]. Feinberg's teachings involve digital cameras equipped with wireless network connectivity, typically compatible with IEEE

802.11 a/b/g standards, facilitating the transfer of image data from the media card to a personal computer or printer. Feinberg, [0005]. Additionally, Feinberg illustrates the uploading of images to an Internet-based computer/storage resource, utilizing a mobile phone. Feinberg, [0049].

669. Second, Kahn teaches offering users the option to "preview" photos, which essentially means displaying thumbnails. Kahn, [0075]. Furthermore, Kahn discloses providing users with an image preview feature, enabling individual image processing. Kahn, [0079]. Specifically, before commencing photo upload to the web-server, at execution path K, the applet displays UI dialog 550 (FIG. 5E), granting access to individual images on the camera. Kahn, [0079], FIG. 5E. Similarly, Feinberg discloses that every full-resolution image captured by the Digital Still Camera (DSC) and stored on the storage device is accompanied by a thumbnail, which is an identical image at a lower resolution. Feinberg, [0133]. These reduced-resolution images are directly accessible by the DSC, allowing users to review and display them, and make decisions about keeping or deleting images. Feinberg, [0133]. Additionally, Feinberg teaches transferring lower resolution versions of all captured images quickly, before performing uploads of the full resolution counterparts. Feinberg, [0091]. Furthermore, in FIG. 4B, Feinberg illustrates that the lower resolution images may include a thumbnail of the digital image being transferred, along with an updated status display showing

progress to date. Feinberg, [0107], [0112], [0140], FIG. 4B (element 50).

670. Third, Kahn teaches offering users the option to "preview" photos captured by the camera on the phone, which includes sending thumbnails across a short-range wireless connection to the mobile phone, which displays the preview images (or thumbnails). Kahn, [0075], [0079], FIG. 5E. In addition, Kahn teaches or suggests that the image server that publishes the images in albums uses thumbnails to display the albums. *See, e.g.*, Kahn, FIG. 6. Notably, Kahn teaches the ability to create a new album when uploading images to the server. Kahn also shows the albums on the server including a thumbnail of at least one image in the album. Thus, Kahn suggests that the server uses a thumbnail to display new albums created by the user for the images that were uploaded. Kahn is silent, however, on how thumbnails are created. Feinberg teaches that it was a known technique—that it was "typical"—to embed thumbnail images "into the full resolution image file header." Feinberg, [0091]. Feinberg provides a solution for transmitting the thumbnails by themselves to the mobile phone for the preview mode. *See, e.g.*, Feinberg, [0091] (describing extracting thumbnails from image files and transmitted). And a POSITA would have recognized the advantage of transmitting the full resolution image with the thumbnails embedded in the image file header for the server to use to generate the newly created album art.

671. Fourth, a POSITA would have further been motivated to modify Kahn

by embedding thumbnails into the image file header to reduce the number of operations performed by the server and by the system as a whole. Because Kahn teaches using preview images, a POSITA would have recognized that the thumbnails used for the preview images would have been created by the camera. First, because a user can delete images stored on the camera from the preview screen in Kahn, a POSITA would have recognized the resource savings of only sending over thumbnails for previewing the images. This way, only a small portion of the image data needs to be sent over the short-range wireless connection, thereby saving bandwidth and increasing speed and user friendliness. Second, a POSITA would have recognized that Kahn teaches that the upload buttons transfer images from the camera to the server. If the mobile phone of Kahn had generated preview images from received full resolution images, the upload buttons would have allowed the transfer of images directly from the phone to the server. As it is, Kahn supports the conclusion that the preview images are thumbnails sent to the phone from the camera without full resolution images.

672. Because the camera creates thumbnails, a POSITA would have recognized that it would have been computationally efficient to send the existing thumbnails to the server, as opposed to requiring the server to spend computational resources to generate thumbnails itself. The server, upon receiving the full resolution images from the phone, could simply extract the thumbnail information

from the image file header for use in creating the album cover.

673. The teachings of Feinberg would have provided the required techniques/details to the users of the mobile phone device in Kahn. Feinberg teaches creating scaled version Feinberg would have allowed to user to create thumbnails of a full resolution image that could be used as "preview" images with lower resolution.

2. Motivation to Combine Kahn-Feinberg with Bluetooth

674. A POSITA would have been motivated to use Bluetooth to wirelessly connect the camera with the mobile phone in Kahn-Feinberg. First, Bluetooth was a well-known technique at the time of Kahn and Feinberg for connecting a mobile phone with a camera. *See, e.g.*, Hiroishi, [0066]-[0067]. A POSITA reviewing Kahn would have known to use such as well-know and ubiquitous short-range wireless communication technology to connect the camera with the mobile phone.

675. In addition, Kahn describes using a stand-alone GPS module to provide GPS information to the camera or mobile phone. *See, e.g.*, Kahn, [0055]. Feinberg contemplates using Bluetooth as a local wireless link to couple a GPS to another communication device. *See, e.g.*, Feinberg, [0041], [0047], [0077]. Based on Feinberg's teachings of Bluetooth, a POSITA would have recognized at a mobile phone, like that in Kahn would have included Bluetooth functionality. A POSITA would have been motivated to use that Bluetooth functionality to also

form a wireless connection between the camera and the phone.

676. A POSITA would have had a reasonable expectation of success implementing Bluetooth. First, Bluetooth was a well-known technology at the time, and a POSITA would have had the requisite skills to implement it. Second, the Bluetooth specification provides ample details to perform all of the Bluetooth operations necessary to establish a connection between two devices, pair the two devices, and communicate data between the two devices.

3. Analysis

677. In Ground 2A, it was established that the combination of Kahn and Bluetooth render each Challenged Claim unpatentable. In that analysis, the "signal to notify" of the claims was mapped onto Kahn's timestamp and related metadata. In this Ground, Feinberg teaches that thumbnails may be included in the header of an object containing photos and thus in this combination, the thumbnails are sent twice. First, they are sent as a preview of the available photos. Second, they are included in the header of the object containing the uploaded photos. In the combination, the thumbnails in the header act as a signal to notify similar to how the timestamp operates as a signal to notify.

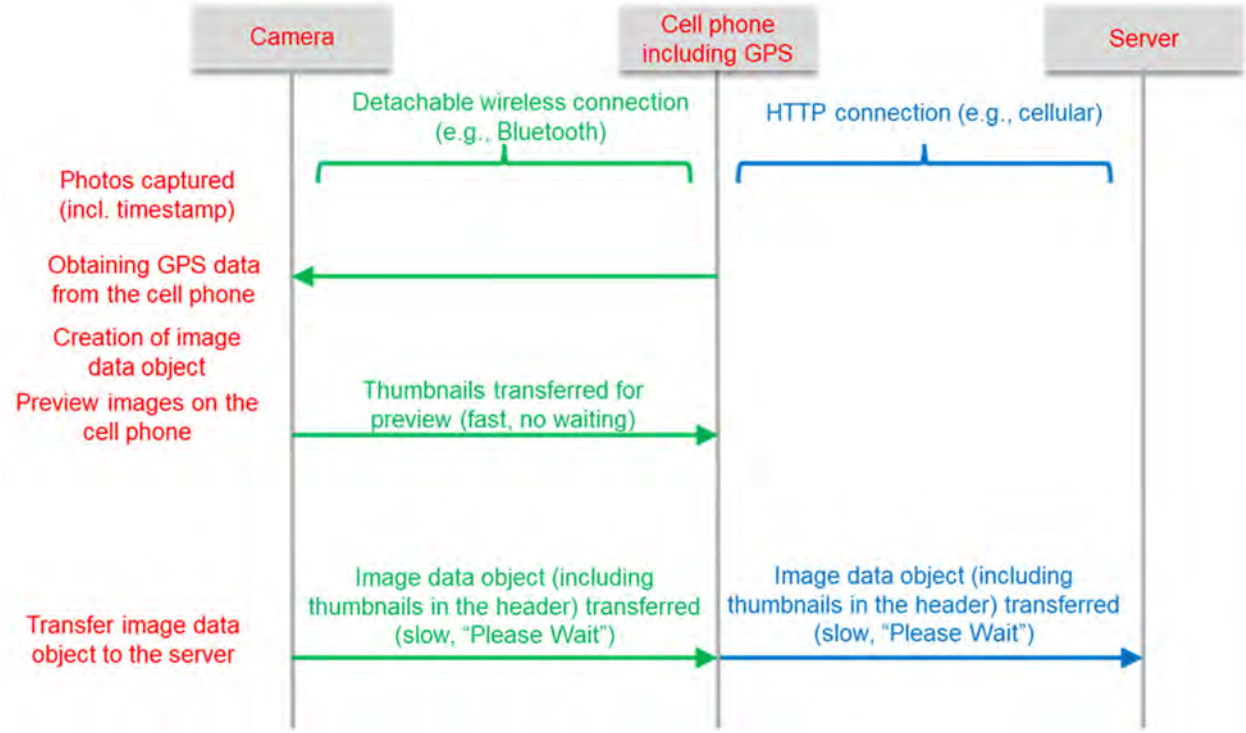
678. A POSITA would have been motivated to implement the teaching of Feinberg so that the thumbnail images are "typically embedded into the full resolution image file header." TTI-1025, [0091]. The inclusion of thumbnails in

the header would not require any additional image processing as Feinberg teaches that "thumbnails are extracted from the image files and transmitted, with no additional image processing." Id.

679. A POSITA would have been motivated to use the thumbnails in the header of the object (or metadata related to the thumbnails) as a signal to the mobile phone software that photos have been retrieved from the camera. For example, the software can count the number of thumbnails included in the header or read a count value that accompanies the thumbnails in the header and use that information as a signal to notify the software that some number of photos have been retrieved.

680. 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.

681. Below is an illustration that shows the high-level flow of the data object in the Kahn-Feinberg combination including the timestamp, full resolution image, and thumbnails.

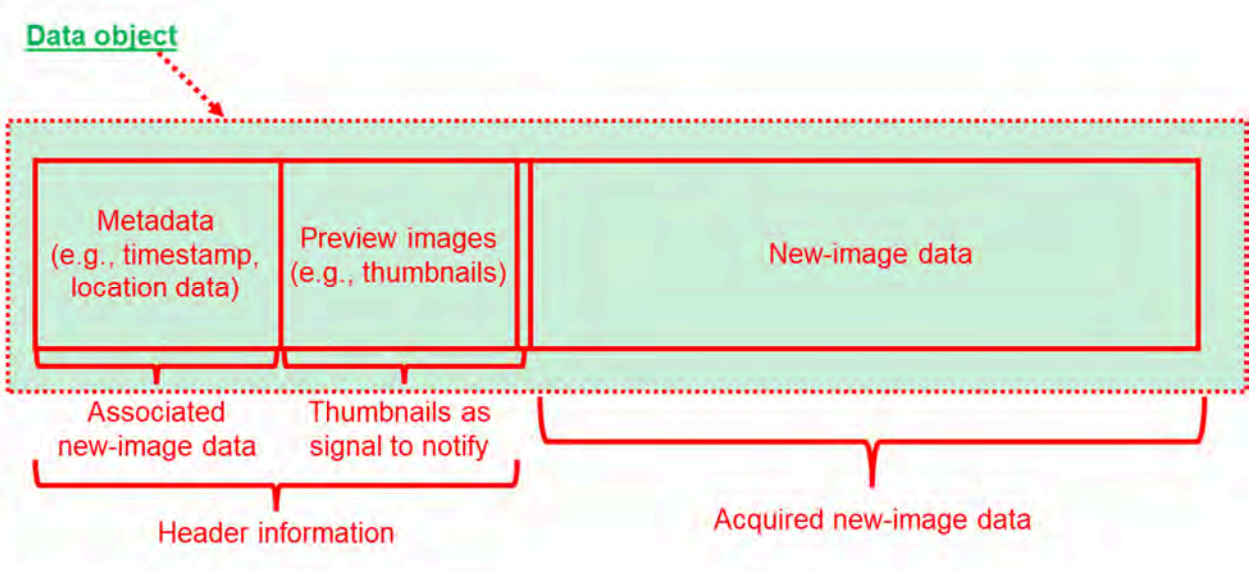


TTI-1017, FIGs. 5A-F, [0070]-[0087].

682. Kahn discloses that the thumbnails can be previewed in screen 550 and there is no wait time shown after selecting preview. TTI-1017, FIG. 5E. Kahn teaches that "[w]hen photos are 'uploaded', they are moved from the camera to the server." *Id.*, FIGs. 5B, 5E, [0063]. In the combination, after the preview thumbnails are provided, either the data objects are transmitted without further prompting from the cellular phone or the camera can wait for a request to transfer the photos. A POSITA would be motivated to provide both options. For example, some users may want the full images as quickly as possible without having to intervene and make a request whereas others would desire to inspect and select only certain pictures.

683. A POSITA would understand that because there is no wait time for previewing thumbnails on the phone as compared to wait time for uploading images to mean that the only thumbnails are transferred from the camera to the phone during preview. Feinberg teaches that the uploaded "thumbnail images (e.g., having 160×120 pixel resolution) are typically embedded into the full resolution image file header." TTI-1025, [0091].

684. A POSITA would thus understand that the thumbnails, full resolution images, and metadata (timestamp, location information) are stored on the camera and uploaded to the server through the phone as a data object. TTI-1017, [0064]. The illustration below shows a new-data object prepared based on the teachings of Kahn-Feinberg combination.



TTI-1017, [0051], [0058], [0062]-[0065], [0098].

685. A POSITA would have understood that creating a new-data object

would include creating preview images (i.e., thumbnails) as disclosed in Kahn. Id., [0075] ("simply "preview" photos"), [0079], FIG. 5E (figure element 550), FIG. 6.

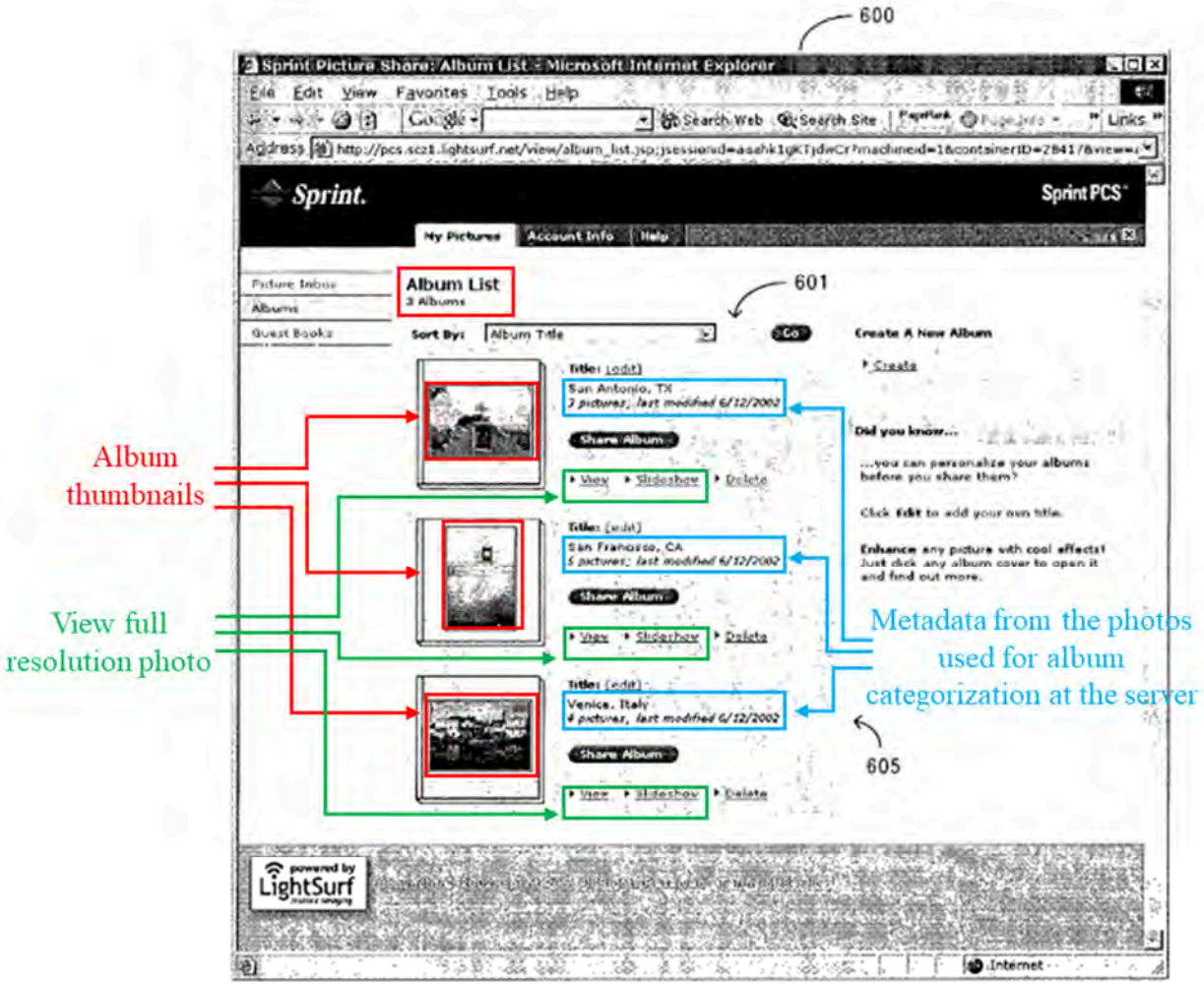


FIG. 6

Id., FIG. 6 (annotated). In FIG. 6, Kahn illustrates, thumbnails being displayed on a "a browser-based interface for accessing one's photos on-line." Id., [0027], [0089].

686. In light of the disclosure presented in Kahn, a POSITA would have

understood that creating a new-data object shares conceptual similarities with the creation of preview images (i.e., thumbnails) and the metadata stored together with the image data serving as mechanisms for transmitting data between devices and signaling events or the availability of new data. Id.; TTI-1017, [0058]-[0059], [0062], [0064]-[0065], [0098]; TTI-1025, [0091].

687. Below is a detailed analysis of each individual limitation::

Claim 1

[1.P] A short-range wireless enabled data capture device, comprising:

688. To the extent the preamble is limiting, The Kahn-Feinberg-Bluetooth combination renders obvious [1.P]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a short-range wireless enabled data capture device. For example, Kahn discloses "an imaging device capable of capturing a plurality of images." Kahn, Abstract, [0018]. Kahn teaches "[a] camera device 310 is a stand-alone unit that is occasionally (or persistently) connected to the host device 320, which may be any device capable of hosting the camera device 310. For example, host device 320 may comprise a cellular phone, a PDA (personal data assistant) with wireless connectivity, or the like.". Kahn, [0055].

689. In FIG. 3, Kahn illustrates a "system 300 [that] includes **a camera device 310**, a host device 320, and a GPS (Global Positioning System) module 325. **The camera device 310 is preferably a wireless camera device**, such as

camera device 100 (shown in FIG. 1A), **that either includes wireless connectivity itself or connects to a local host with wireless connectivity.**" Kahn, [0055].

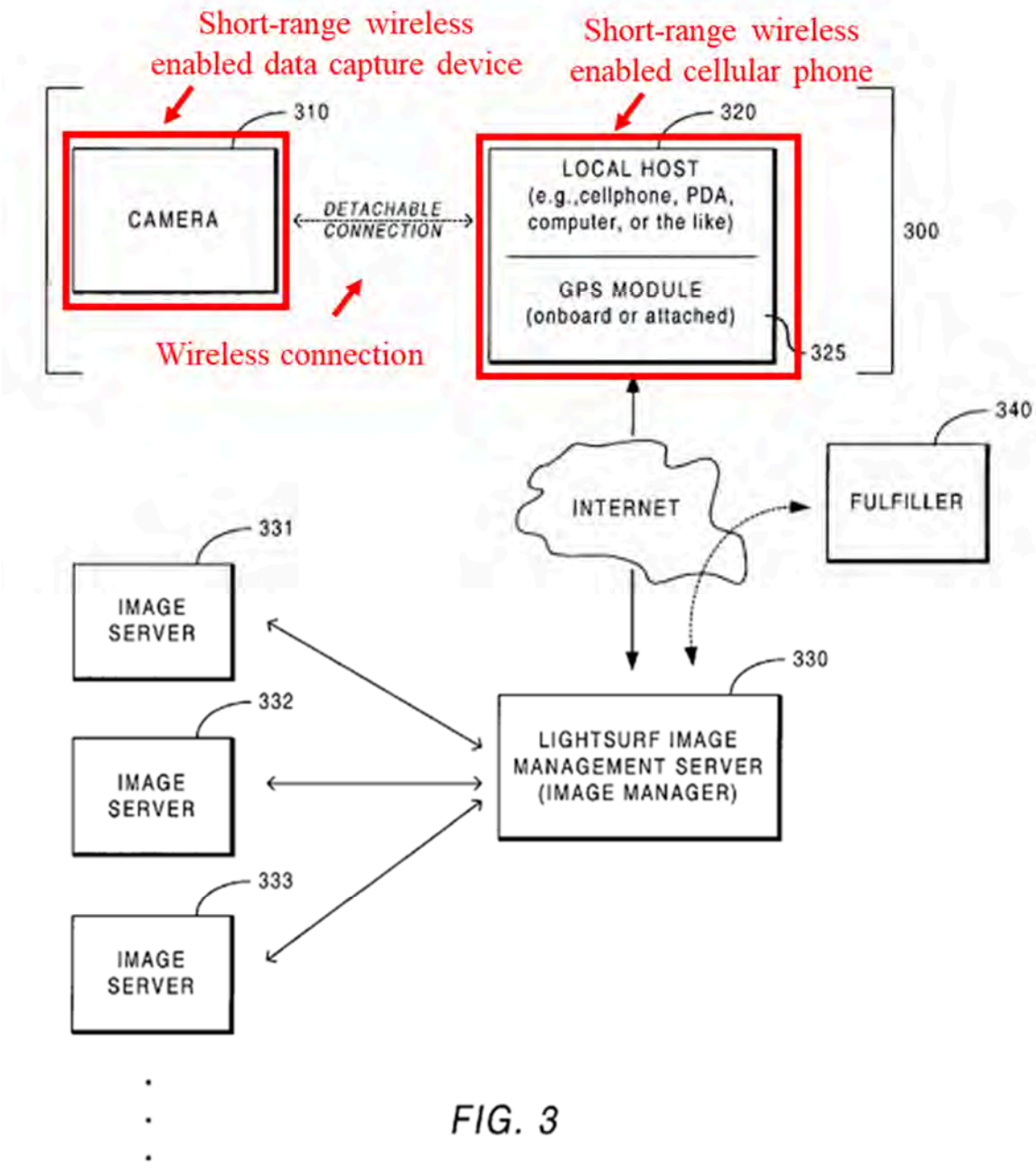


FIG. 3

Kahn, FIG. 3 (annotated). Kahn, [0023] ("FIG. 3 is a high-level block diagram illustrating the basic components that comprise the environment in which the present embodiment may be implemented.")

690. While Kahn does not expressly mention the range of the wireless connection between a camera and a cell phone, it suggests a "detachable connection" and in some instances, "cableless direct connection." Kahn, FIG. 3, [0045]. Considering these connection characteristics, a POSITA would have understood that the connection between a camera and a cell phone would likely be a short-range wireless connection.

[1.1] a memory device;

691. The Kahn-Feinberg-Bluetooth combination renders obvious [1.1]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a memory device. For example, Kahn teaches "captured image data is transferred over the system bus 130 to the computer 140 which performs various image processing functions on the image data before storing it in its internal memory." Kahn, [0035].

692. Kahn discloses a "system 300 [that] includes a camera device 310, a host device 320, and a GPS (Global Positioning System) module 325. The camera device 310 is preferably a wireless camera device, such as camera device 100 (shown in FIG. 1A), that either includes wireless connectivity itself or connects to a local host with wireless connectivity." Kahn, [0055], FIGs. 1A, 3.

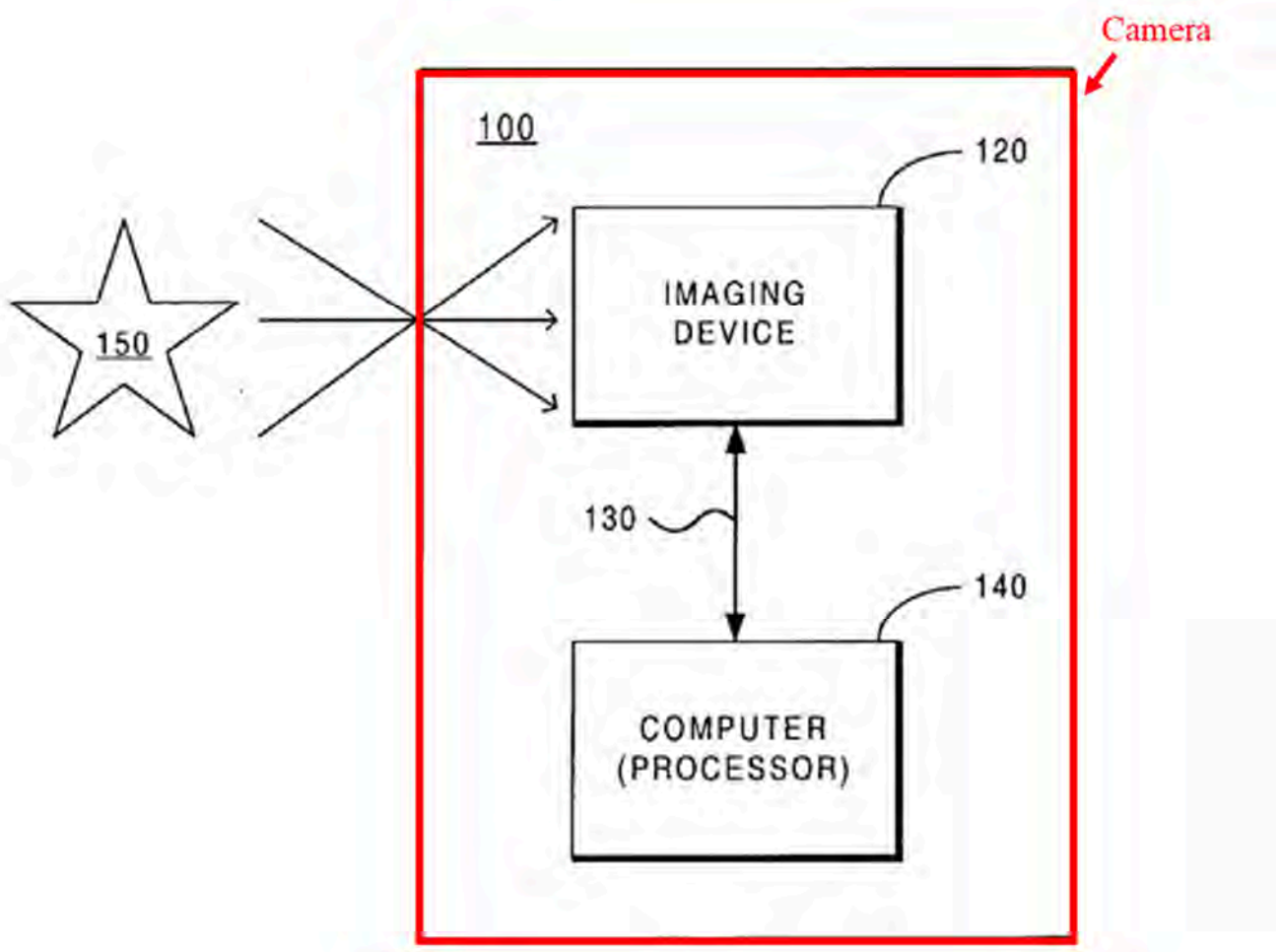


FIG. 1
(PRIOR ART)

Kahn, FIG. 1 (annotated). Kahn, [0020] ("FIG. 1 is a very general block diagram of a digital camera suitable for implementing the present invention.")

693. As below above in FIG. 2B, Kahn illustrates "[a] conventional onboard processor or computer 140 is provided for directing the operation of the digital camera 100 and processing image data captured on the imaging device 120.

FIG. 2B is a block diagram of the processor or computer 140. As shown, the system bus 130 provides connection paths between the imaging device 120, an (optional) power management 262, a processor (CPU) 264, a random-access memory (RAM) 266, an input/output (I/O) controller 280, a non-volatile memory 282, a removable memory interface 283, and a liquid crystal display (LCD) controller 290. Removable memory 284 connects to the system bus 130 via the removable memory interface 283. Alternately, the camera 100 (and therefore the onboard computer 140) may be implemented without the removable memory 284 or the removable memory interface 283." Kahn, [0042].

694. Further, Kahn discloses that "[t]he digital camera 100 includes several memory components. **The memory (RAM) 266 is a contiguous block of dynamic memory that may be selectively allocated to various storage functions.** Dynamic random-access memory is available from a variety of vendors, including, for instance, Toshiba of Japan, Micron Technology of Boise, Id., Hitachi of Japan, and Samsung Electronics of South Korea. **The non-volatile memory 282, which may typically comprise a conventional read-only memory or flash memory, stores a set of computer-readable program instructions to control the operation of the camera 100. The removable memory 284 serves as an additional image data storage area and may include a non-volatile device, readily removable and replaceable by a camera 100 user via the removable**

memory interface 283. Thus, a user who possesses several removable memories 284 may replace a full removable memory 284 with an empty removable memory 284 to effectively expand the picture-taking capacity of the camera 100. The removable memory 284 is typically implemented using a flash disk. Available vendors for flash memory include, for example, SanDisk Corporation of Sunnyvale, Calif. and Sony of Japan. Those skilled in the art will appreciate that the digital camera 100 may incorporate other memory configurations and designs that readily accommodate the image capture and processing methodology of the present invention." Kahn, [0044].

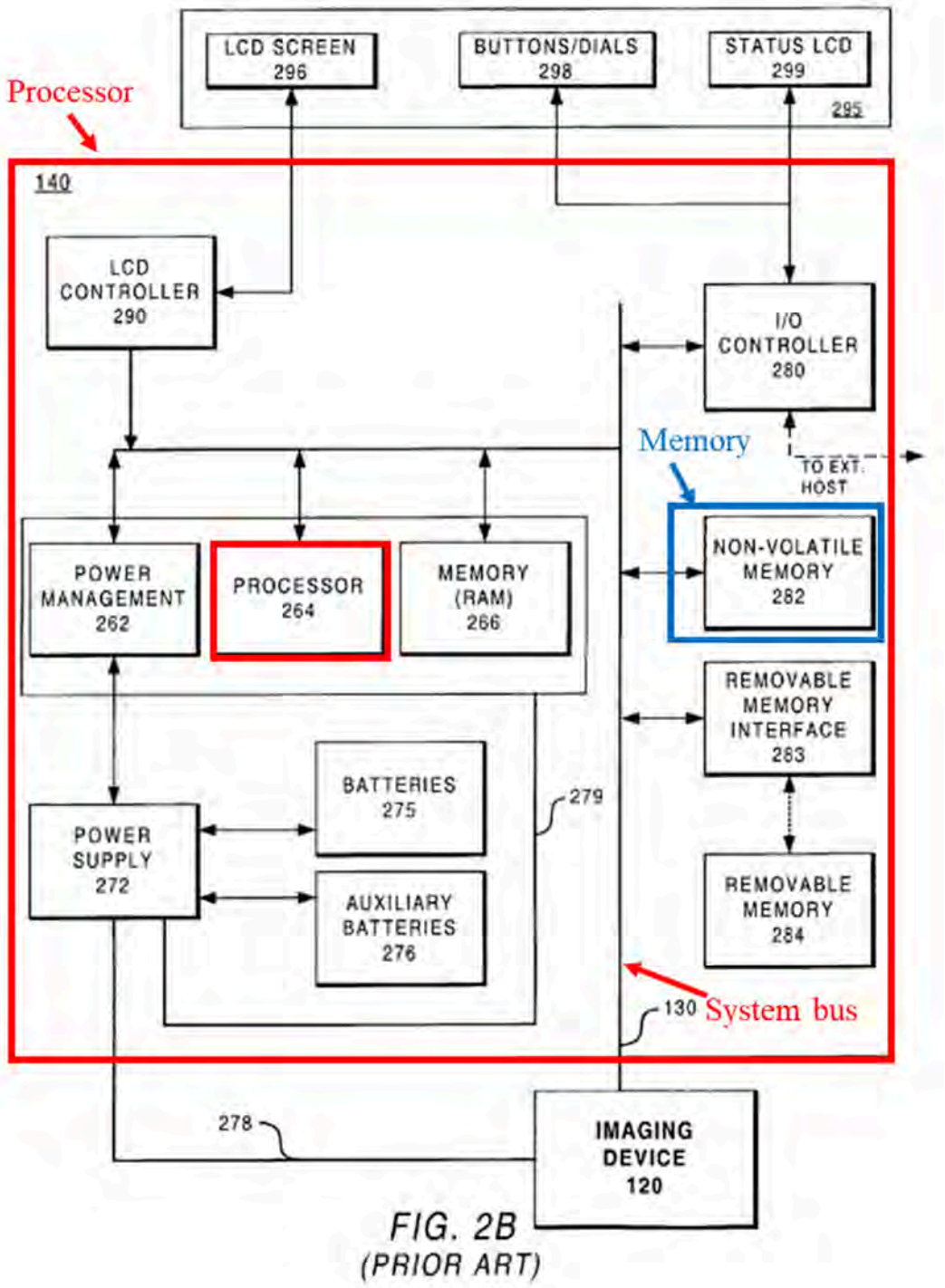


FIG. 2B
(PRIOR ART)

Kahn, FIG. 2B (annotated). Kahn, [0022] ("FIG. 2B is a block diagram of the processor or computer used for the digital imaging device of FIG. 2A.")

[1.2] a processor coupled to said memory device;

695. The Kahn-Feinberg-Bluetooth combination renders obvious [1.2]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a processor coupled to said memory device. For example, Kahn discloses "the digital camera 100 comprises an imaging device 120, a system bus 130, and a processor or computer 140 (e.g., microprocessor-based unit)." Kahn, [0033]. See also, id., [0034]-[0035], [0045].

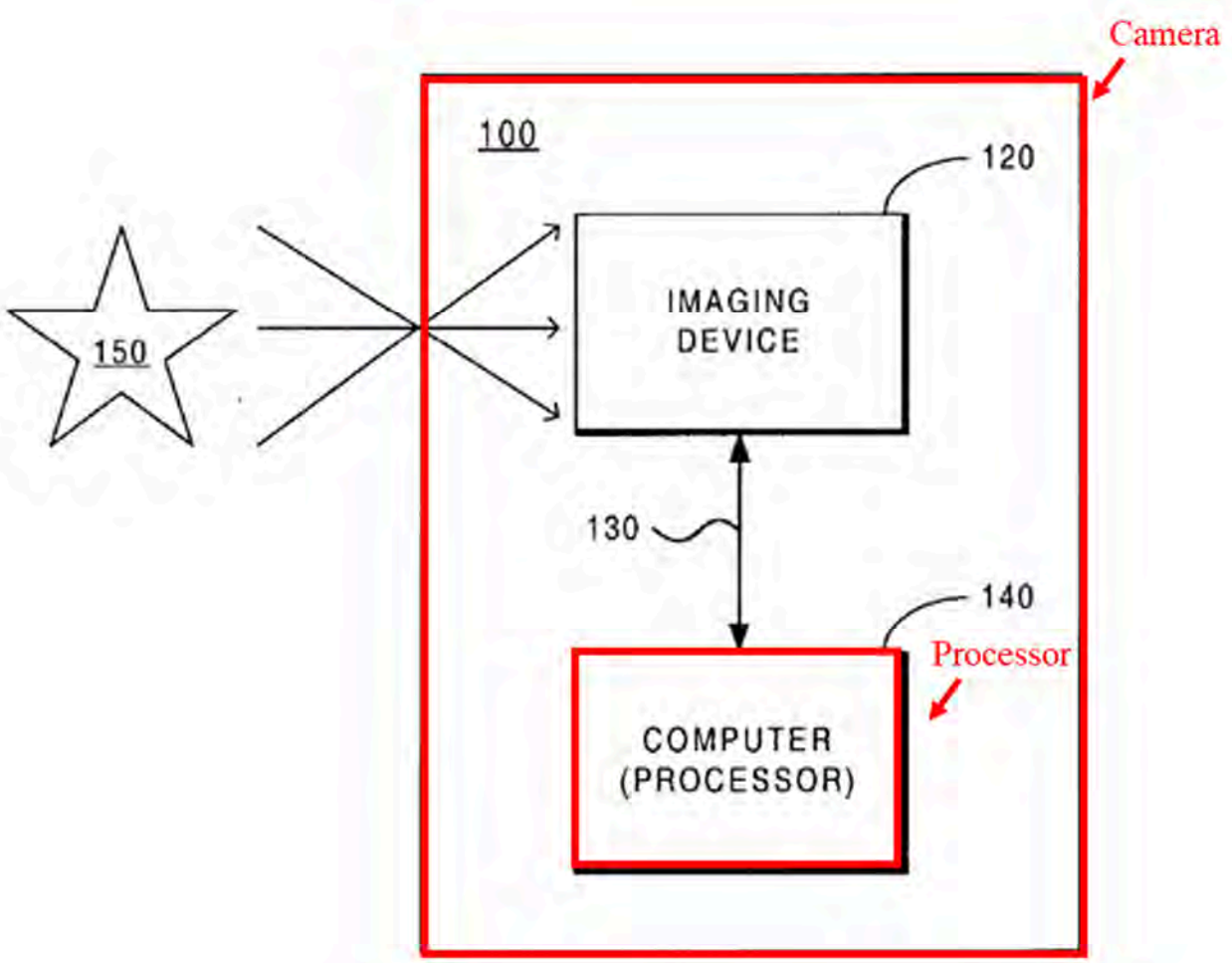
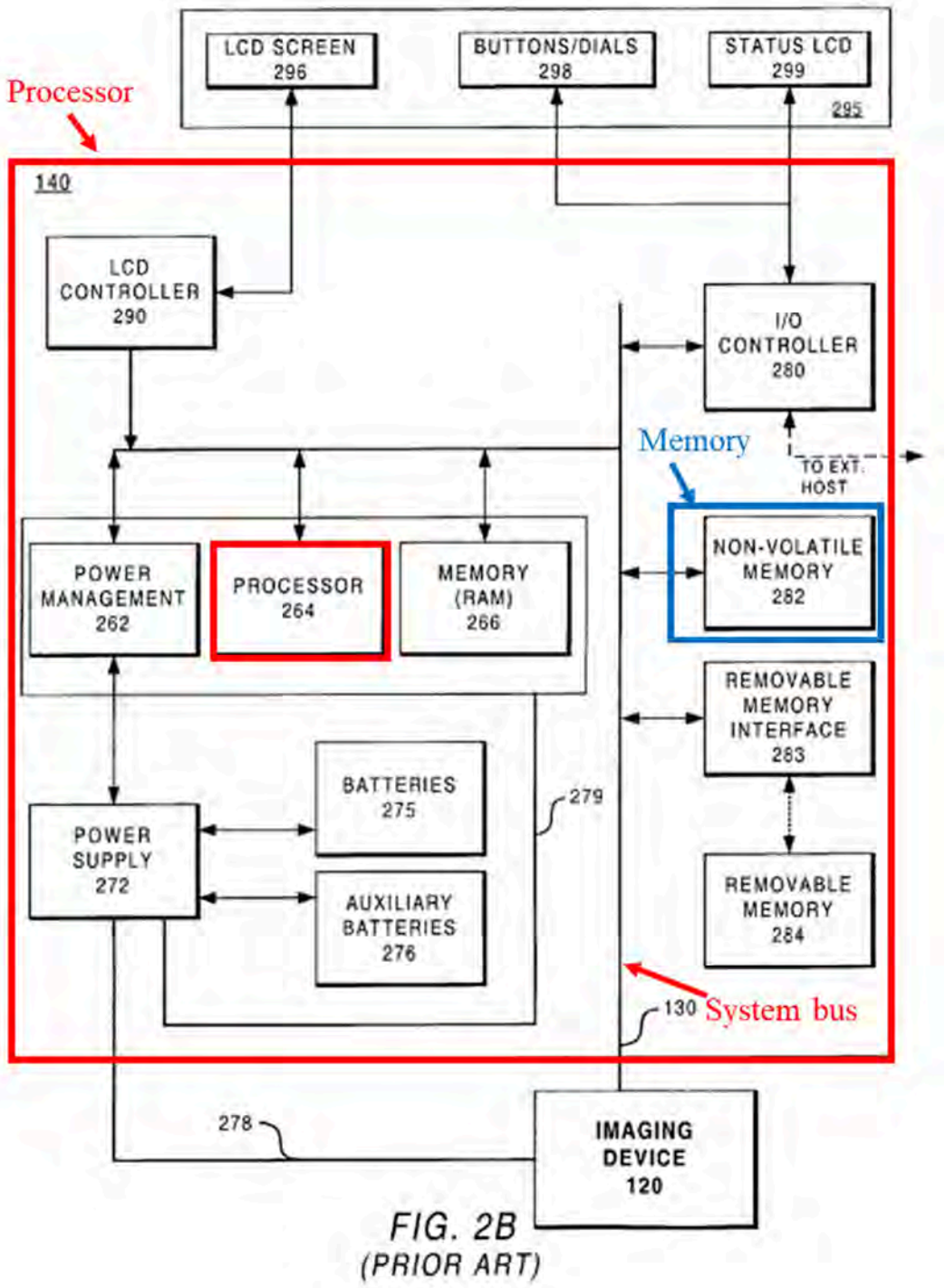


FIG. 1
(PRIOR ART)

Kahn, FIG. 1 (annotated). Kahn, [0020] ("FIG. 1 is a very general block diagram of a digital camera suitable for implementing the present invention.")

696. FIG 2B. in Kahn shows processor 264 coupled to memories via bus 130 including memory (RAM) 266, non-volatile memory 262, and removable memory 284 (via interface 283). Kahn, [0042) ("[a] conventional onboard

processor or computer 140 is provided for directing the operation of the digital camera 100 and processing image data captured on the imaging device 120. FIG. 2B is a block diagram of the processor or computer 140 …**the system bus 130 provides connection paths between** the imaging device 120, an (optional) power management 262, **a processor (CPU) 264**, a random-access memory (RAM) 266, an input/output (I/O) controller 280, **a non-volatile memory 282**, a removable memory interface 283, and a liquid crystal display (LCD) controller 290.").



Kahn, FIG. 2B (annotated). Kahn, [0022] ("FIG. 2B is a block diagram of the processor or computer used for the digital imaging device of FIG. 2A.")

697. Further, Kahn discloses, "[t]he processor (CPU) 264 typically

includes a conventional processor device (e.g., microprocessor) for controlling the operation of camera 100. Implementation of the processor 264 may be accomplished in a variety of different ways. For instance, the processor 264 may be implemented as a microprocessor (e.g., MPC823 microprocessor, available from Motorola of Schaumburg, Ill.) with DSP (digital signal processing) logic blocks, memory control logic blocks, video control logic blocks, and interface logic. Alternatively, the processor 264 may be implemented as a "camera on a chip (set)" using, for instance, a Raptor II chipset (available from Conextant Systems, Inc. of Newport Beach, Calif.), a Sound Vision Clarity 2, 3, or 4 chipset (available from Sound Vision, Inc. of Wayland, Mass.), or similar chipset that integrates a processing core with image processing periphery. Processor 264 is typically capable of concurrently running multiple software routines to control the various processes of camera 100 within a multithreaded environment." Kahn, [0043].

[1.3]-[1.5] a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone,
wherein establishing the short-range paired wireless connection comprises cryptographically authenticating identity of the short-range wireless enabled cellular phone, and
wherein establishing the short-range paired wireless connection further comprises the short-range wireless enabled data capture device using an association protocol;

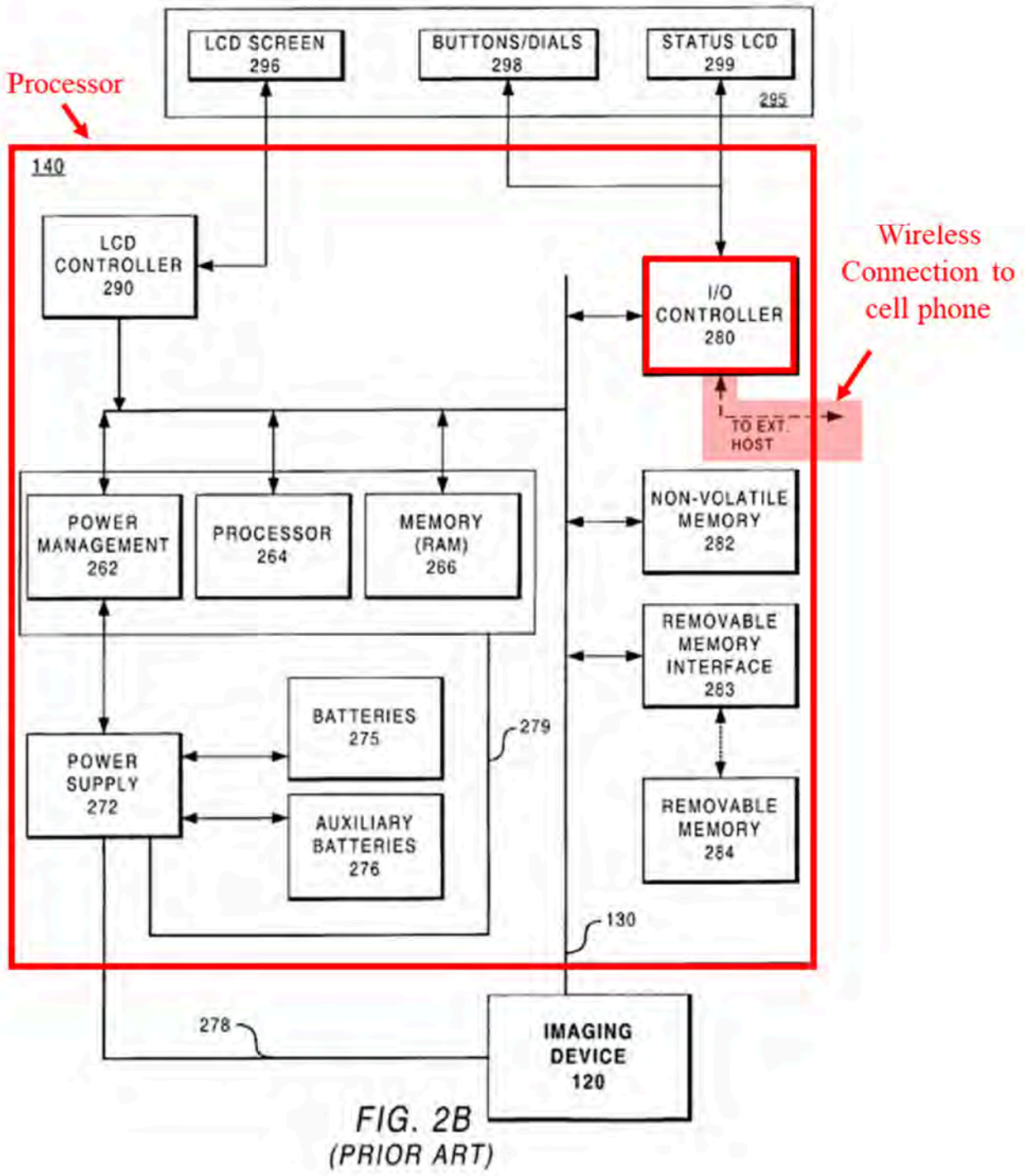
698. The Kahn-Feinberg-Bluetooth combination renders obvious [1.3]-[1.5]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a short-range

wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone, wherein establishing the short-range paired wireless connection comprises cryptographically authenticating identity of the short-range wireless enabled cellular phone, and wherein establishing the short-range paired wireless connection further comprises the short-range wireless enabled data capture device using an association protocol.

This limitation is broken down into constituent steps below:

[1.3] a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone;

699. For example, Kahn discloses "[t]he digital camera 100 also typically includes several interfaces for communication with a camera user or with other systems and devices. For example, **the I/O controller 280 is an interface device allowing communications to and from the computer 140. The I/O controller 280 permits an external host, such as a cell phone**, personal digital assistant (PDA), computer, or the like (not shown), **to connect to and communicate with the computer 140**." Kahn, [0045]. "[A] digital camera that includes occasional [wireless] connectivity to a local host device (e.g., GPS-enabled cell phone, personal digital assistant (PDA), laptop computer, or the like).". Kahn, [0030].



Kahn, FIG. 2B (annotated). Kahn, [0022] ("FIG. 2B is a block diagram of the processor or computer used for the digital imaging device of FIG. 2A.")

700. In FIG. 3, Kahn illustrates a "system 300 [that] includes **a camera**

device 310, a host device 320, and a GPS (Global Positioning System) module 325. **The camera device 310 is preferably a wireless camera device**, such as camera device 100 (shown in FIG. 1A), **that either includes wireless connectivity itself or connects to a local host with wireless connectivity.** 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, which may be any device capable of hosting the camera device 310. For example, host device 320 may comprise a cellular phone, a PDA (personal data assistant) with wireless connectivity, or the like." Kahn, [0055].

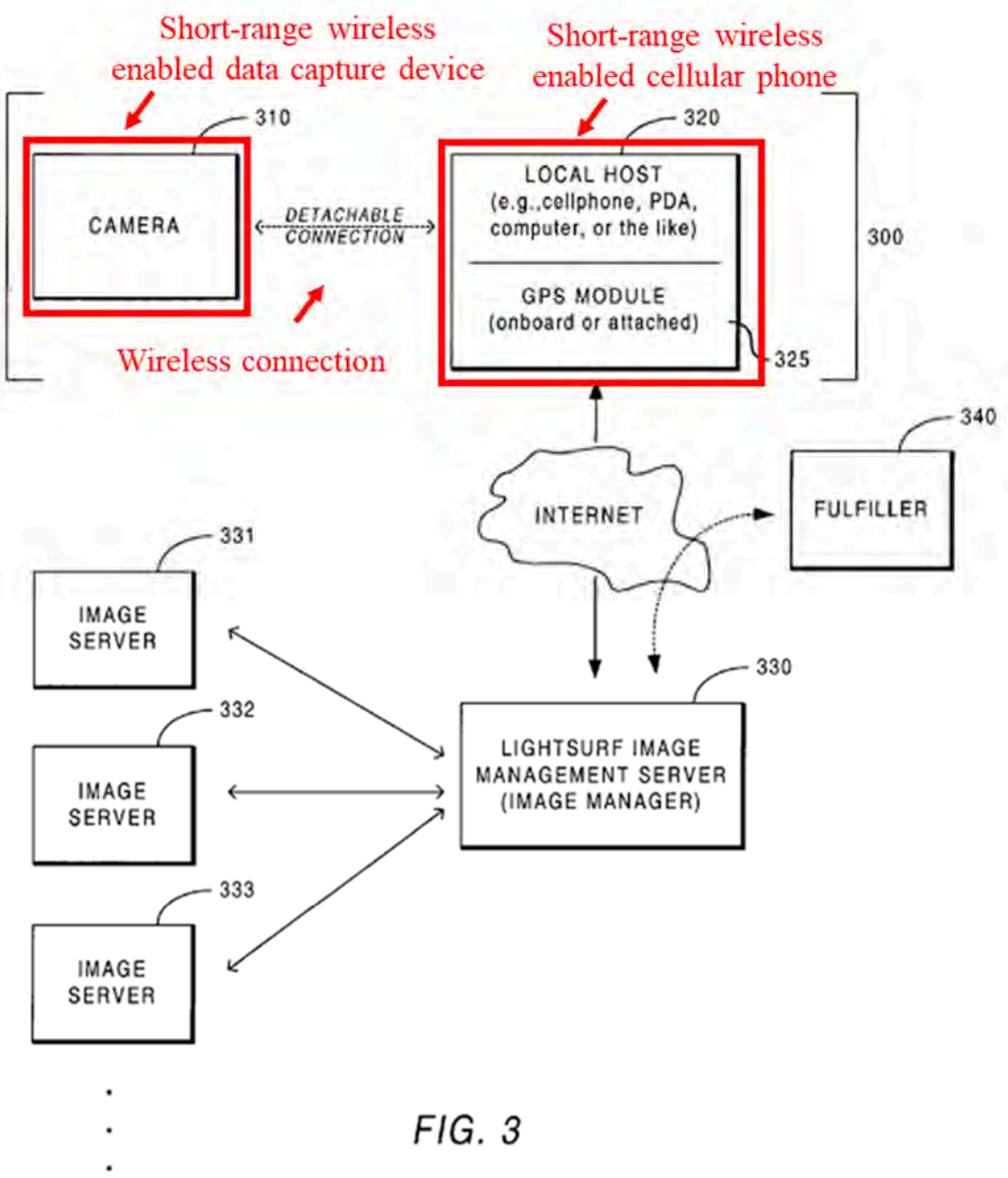


FIG. 3

Kahn, FIG. 3 (annotated). Kahn, [0023] ("FIG. 3 is a high-level block diagram illustrating the basic components that comprise the environment in which the present embodiment may be implemented.")

701. While Kahn does not expressly mention the range of the wireless

connection between a camera and a cell phone, it suggests a "detachable connection" and in some instances, "cableless direct connection." Kahn, FIG. 3, [0045]. Considering these connection characteristics, a POSITA would have understood that the connection between a camera and a cell phone would likely be a short-range wireless connection.

[1.4] wherein establishing the short-range paired wireless connection comprises cryptographically authenticating identity of the short-range wireless enabled cellular phone, and

702. As mentioned above (supra [1.3]) Kahn teaches a "detachable connection" and in some instances, "cableless direct connection." Kahn, FIG. 3, [0045]. While Kahn does not expressly specify the type of communication for the wireless detachable connection between the camera and the cell phone, a POSITA would find it as an obvious choice to utilize Bluetooth, which was a commonly used technique to establish a "detachable connection", "cableless direct connection." Kahn, FIG. 3, [0045]. Bluetooth was a well-known wireless communication technique before the alleged Critical Date. Bluetooth could establish short-range paired wireless communication between a camera and a cell phone.

703. Although Kahn does not expressly disclose the camera cryptographically authenticating the identity of the phone, it would have been obvious to a POSITA to modify Kahn to include this limitation because a POSITA

would have been motivated to implement Bluetooth as the standard for communications between the camera 310 and the cell phone 320. *See, e.g.*, Kahn, [0045], [0096]. Particularly, a POSITA would have known that Bluetooth pairing between any two devices (for example, a camera and a cell) would involve the use of such cryptographic encryption keys which was a standard and well known part of the Bluetooth specification. For example, as discussed in the Bluetooth Core Specification V2.1, pairing between Bluetooth devices includes the generation and exchange of initialization keys created from a PIN, a random number, and a Bluetooth Device Address (BD_ADDR):

704. Referring to Bluetooth Core Specification 2.1 (July 2007), the pairing processes uses the BD_ADDR to form the initialization key (Kinit):

4.2.2 Pairing

When two devices do not have a common link key an initialization key (K_{init}) shall be created using either the pairing or Secure Simple Pairing procedures. When pairing is used, K_{init} shall be created based on a PIN, and a random number and a BD_ADDR. K_{init} shall be created as specified in [Part H] Section 6.3 on page 885. When both devices have calculated K_{init} the link key shall be created, and a mutual authentication is performed. The pairing procedure starts with a device sending an LMP_in_rand PDU; this device is referred to as the "initiating LM" or "initiator" in Section 4.2.2.1 on page 242 - Section 4.2.2.5 on page 245. The other device is referred to as the "responding LM" or "responder". The PDUs used in the pairing procedure are:

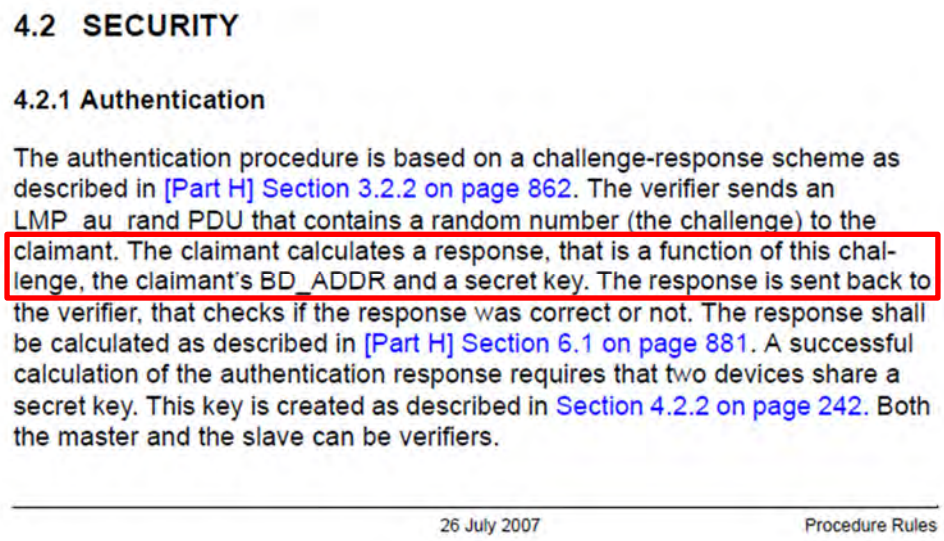
M/O	PDU	Contents
M	LMP_in_rand	random number
M	LMP_au_rand	random number
M	LMP_sres	authentication response
M	LMP_comb_key	random number
M	LMP_unit_key	key

Table 4.14: Pairing PDUs

All sequences described in Section 4 on page 223, including the mutual authentication after the link key has been created, shall form a single transaction. The transaction ID from the first LMP_in_rand shall be used for all subsequent sequences.

See, e.g., Bluetooth Core Specification, 412.

705. In another example, the Bluetooth Core specification describes the process for establishing a secure pairing as well as the obvious reasons behind secure pairing:



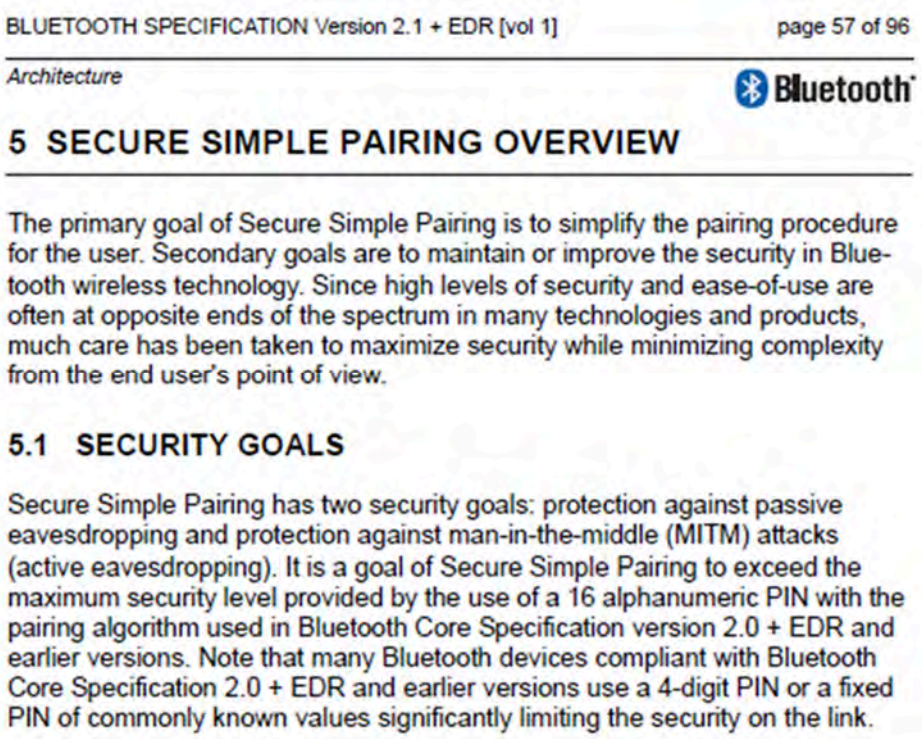
4.2 SECURITY

4.2.1 Authentication

The authentication procedure is based on a challenge-response scheme as described in [Part H] Section 3.2.2 on page 862. The verifier sends an LMP_au_rand PDU that contains a random number (the challenge) to the claimant. The claimant calculates a response, that is a function of this challenge, the claimant's BD_ADDR and a secret key. The response is sent back to the verifier, that checks if the response was correct or not. The response shall be calculated as described in [Part H] Section 6.1 on page 881. A successful calculation of the authentication response requires that two devices share a secret key. This key is created as described in Section 4.2.2 on page 242. Both the master and the slave can be verifiers.

See, e.g., Bluetooth Core Specification, 411. The Bluetooth core specification describes using BD_ADDR which represents Bluetooth device address. The BD_ADDR is a unique identifier that cryptographic authentication authenticates the identity of the connected device (for example authenticating between camera and cell phone while Bluetooth connection is being established.)

706. In another example, the Bluetooth Core specification describes a second process for establishing a secure pairing as well as the obvious reasons behind secure pairing:



BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 1] page 57 of 96

Architecture

Bluetooth

5 SECURE SIMPLE PAIRING OVERVIEW

The primary goal of Secure Simple Pairing is to simplify the pairing procedure for the user. Secondary goals are to maintain or improve the security in Bluetooth wireless technology. Since high levels of security and ease-of-use are often at opposite ends of the spectrum in many technologies and products, much care has been taken to maximize security while minimizing complexity from the end user's point of view.

5.1 SECURITY GOALS

Secure Simple Pairing has two security goals: protection against passive eavesdropping and protection against man-in-the-middle (MITM) attacks (active eavesdropping). It is a goal of Secure Simple Pairing to exceed the maximum security level provided by the use of a 16 alphanumeric PIN with the pairing algorithm used in Bluetooth Core Specification version 2.0 + EDR and earlier versions. Note that many Bluetooth devices compliant with Bluetooth Core Specification 2.0 + EDR and earlier versions use a 4-digit PIN or a fixed PIN of commonly known values significantly limiting the security on the link.

See, e.g., Bluetooth Core Specification V2.1, 131.

707. The Bluetooth Core Specification also describes implementation of security at both the link layer and the application layer:

1 SECURITY OVERVIEW

Bluetooth wireless technology provides peer-to-peer communications over short distances. In order to provide usage protection and information confidentiality, the system provides security measures both at the application layer and the link layer. These measures are designed to be appropriate for a peer environment. This means that in each device, the authentication and encryption routines are implemented in the same way. Four different entities are used for maintaining security at the link layer: a Bluetooth device address, two secret keys, and a pseudo-random number that shall be regenerated for each new transaction. The four entities and their sizes are summarized in Table 1.1.

Entity	Size
BD_ADDR	48 bits
Private user key, authentication	128 bits
Private user key, encryption configurable length (byte-wise)	8-128 bits
RAND	128 bits

Table 1.1: Entities used in authentication and encryption procedures.

The Bluetooth device address (BD_ADDR) is the 48-bit address. The BD_ADDR can be obtained via user interactions, or, automatically, via an inquiry routine by a device.

The secret keys are derived during initialization and are never disclosed. The encryption key is derived from the authentication key during the authentication process. For the authentication algorithm, the size of the key used is always 128 bits. For the encryption algorithm, the key size may vary between 1 and 16 octets (8 - 128 bits). The size of the encryption key is configurable for two reasons. The first has to do with the many different requirements imposed on cryptographic algorithms in different countries – both with respect to export regulations and official attitudes towards privacy in general. The second reason is to facilitate a future upgrade path for the security without the need of a costly redesign of the algorithms and encryption hardware; increasing the effective key size is the simplest way to combat increased computing power at the opponent side.

See, e.g., Bluetooth Specification V2.1, 1025.

7 SECURE SIMPLE PAIRING

The Secure Simple Pairing security functions and procedures are described in this section. In addition, a cryptographic analysis of each procedure is provided.

There are five phases of Secure Simple Pairing:

- Phase 1: Public key exchange
- Phase 2: Authentication Stage 1
- Phase 3: Authentication Stage 2
- Phase 4: Link key calculation
- Phase 5: LMP Authentication and Encryption

Phases 1, 3, 4 and 5 are the same for all protocols whereas phase 2 (Authentication Stage 1) is different depending on the protocol used. Distributed through these five phases are 13 steps.

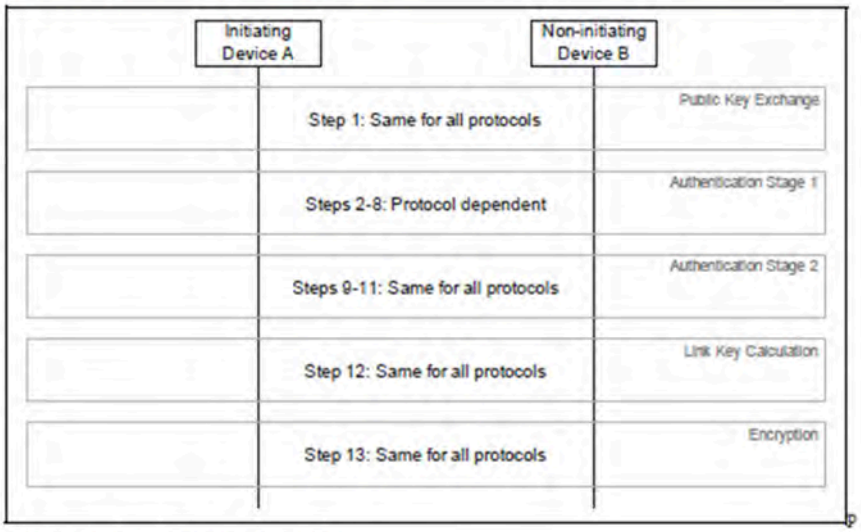


Figure 7.1: Simple Pairing Security Phases

Bluetooth Core Specification, 1058. The Bluetooth core specification describes "Secure Simple Pairing security functions and procedures" between connected devices.

708. Cryptographic authentication between wireless devices like a digital camera and cellular phone was routine at the time of the invention. Indeed,

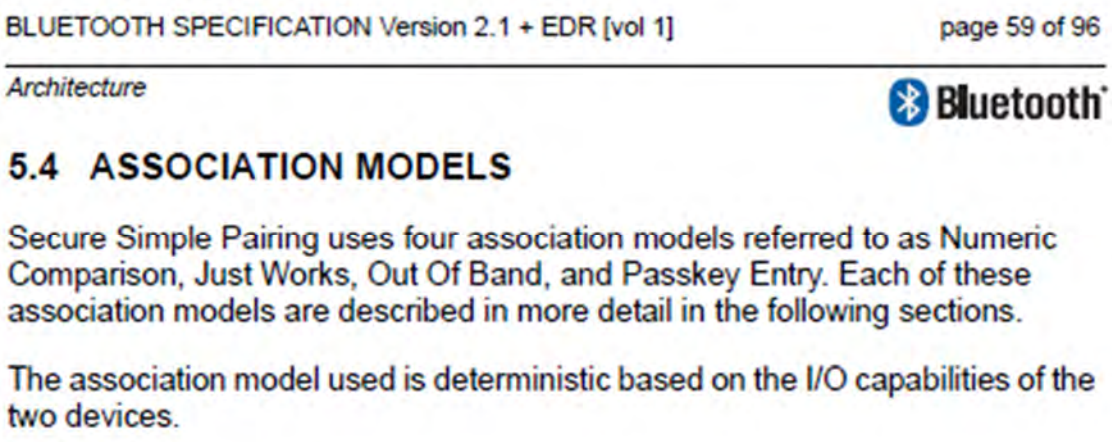
cryptographic authentication was part of the Bluetooth standard for years before the alleged Critical Date. See section V.B.

709. A POSITA would have understood the basic motivation for using cryptographic authentication: to ensure that each device is communicating with its intended recipient and that information is protected from outsiders when transmitted between devices. A POSITA would have found this benefit directly applicable to the system disclosed Kahn, because it would have ensured the secure transmission of image files and related data between the two devices. Kahn teaches that the camera and phone implement a "cableless direct connection" and wireless "detachable connection," a POSITA would have found it obvious to implement Bluetooth as the preferred data transmission mechanism, so there would not have been any unexpected result if the camera and phone were configured to cryptographically authenticate each other.

710. A POSITA would have understood that Bluetooth is the short-range paired wireless connection that comprises the short-range wireless enabled data capture device using an association protocol.

[1.5] wherein establishing the short-range paired wireless connection further comprises the short-range wireless enabled data capture device using an association protocol;

711. A POSITA would have understood and implemented the association models discloses in the Bluetooth specification.



BLUETOOTH SPECIFICATION Version 2.1 + EDR [vol 1] page 59 of 96

Architecture

5.4 ASSOCIATION MODELS

Secure Simple Pairing uses four association models referred to as Numeric Comparison, Just Works, Out Of Band, and Passkey Entry. Each of these association models are described in more detail in the following sections.

The association model used is deterministic based on the I/O capabilities of the two devices.

See, e.g., Bluetooth Specification V2.1, 133.

5.4.5 Association Model Overview

The following diagram shows Secure Simple Pairing from the point of view of the technology used for discovery and then the different association possibilities.

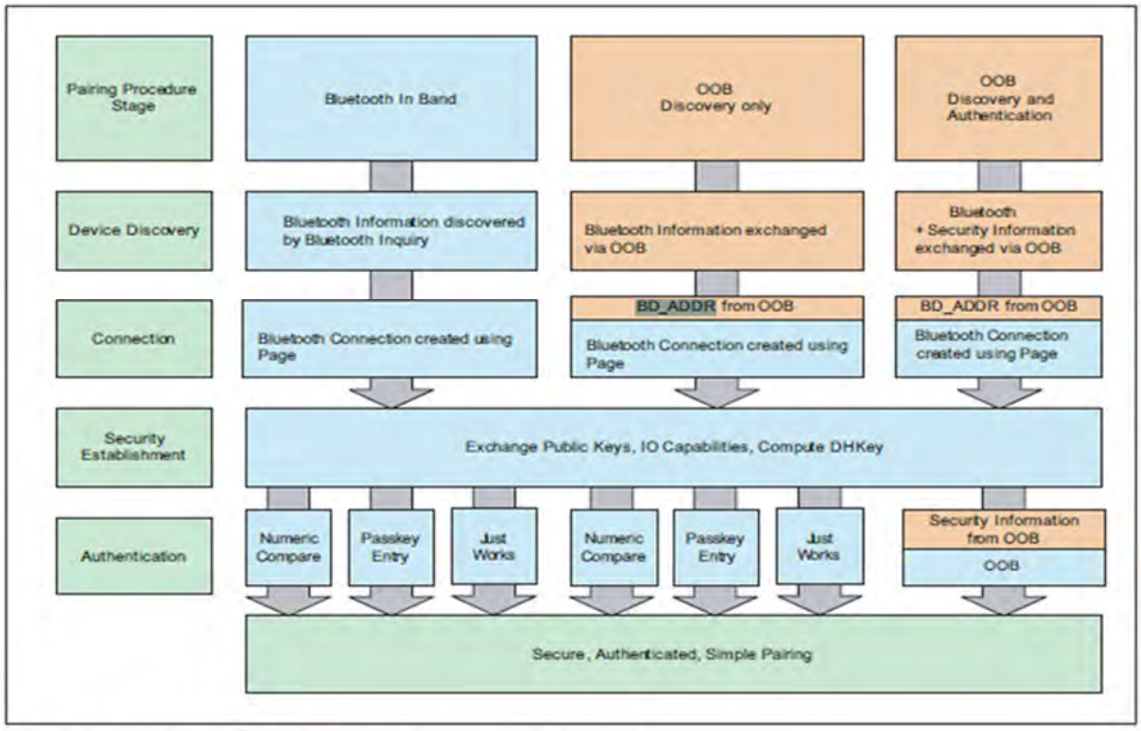


Figure 5.1: Secure Simple Pairing Association Models

See, e.g., Bluetooth Specification V2.1, 135.

[1.6] a data capture circuitry;

712. The Kahn-Feinberg-Bluetooth combination renders obvious [1.6]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a data capture circuitry. For example, Kahn teaches that the camera 100 comprises an "imaging device 120 [which] operates, in essence, by capturing light reflected from the object 150 and transforming that light into image data." Kahn, [0035]. Particularly, "the imaging

device 120 captures an image of the object 150 via reflected light impacting the image sensor 230 along optical path 220 ." Kahn, [0038]. In FIG. 2A, Kahn illustrates "the imaging device 120 compris[ing] a lens 210 having an iris, one or more filter(s) 215 , an image sensor 230 (e.g., CMOS, CCD, or the like), a focus mechanism (e.g., motors) 241 , a timing circuit 242 , a signal processor 251 (e.g., analog signal processor), an analog-to-digital (A/D) converter 253 , and an interface 255 ." Kahn, [0037].

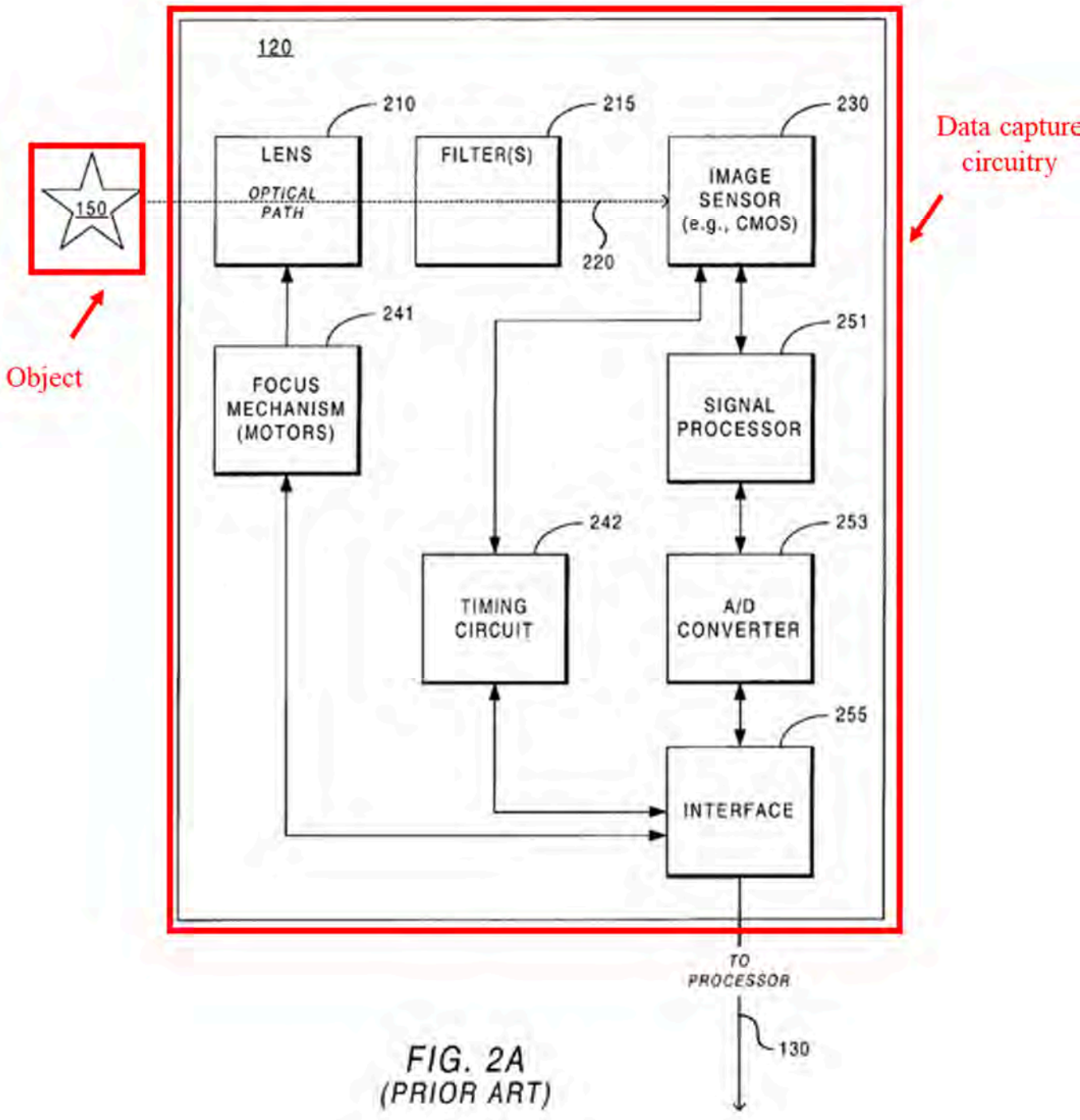


FIG. 2A
(PRIOR ART)

Kahn, FIG. 2A (annotated). Kahn, [0021] ("FIG. 2A is a block diagram of a conventional digital imaging device.")

[1.7]-[1.8] said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;

713. The Kahn-Feinberg-Bluetooth combination renders obvious [1.7]-[1.8]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone.

This limitation is broken down into constituent steps below:

[1.7] said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry,

714. For example, Kahn teaches the computer 140 serves as the central controller for the imaging device 120, directing its actions and timing (Kahn, [0034] ("the computer 140 controls the imaging device 120 by, in effect, telling it what to do and when.")). Through the system bus 130, "the computer 140 [issues] commands [to] the imaging device 120 … to capture an image representing the object 150." Kahn, [0035]. Specifically, Kahn states, "[a] conventional onboard processor or computer 140 is provided for directing the operation of the digital camera 100 and processing image data captured on the imaging device 120."

Kahn, [0042]. In FIG. 2B, Kahn illustrates "a block diagram of the processor or computer 140" comprising a dedicated "a processor (CPU) 264," indicating that "[t]he processor (CPU) 264 typically includes a conventional processor device (e.g., microprocessor) for controlling the operation of camera 100." Kahn, [0042]-[0043]. A POSITA would have understood that the processor 140 is configured to acquire image captured (new-data) by the imaging device 120.

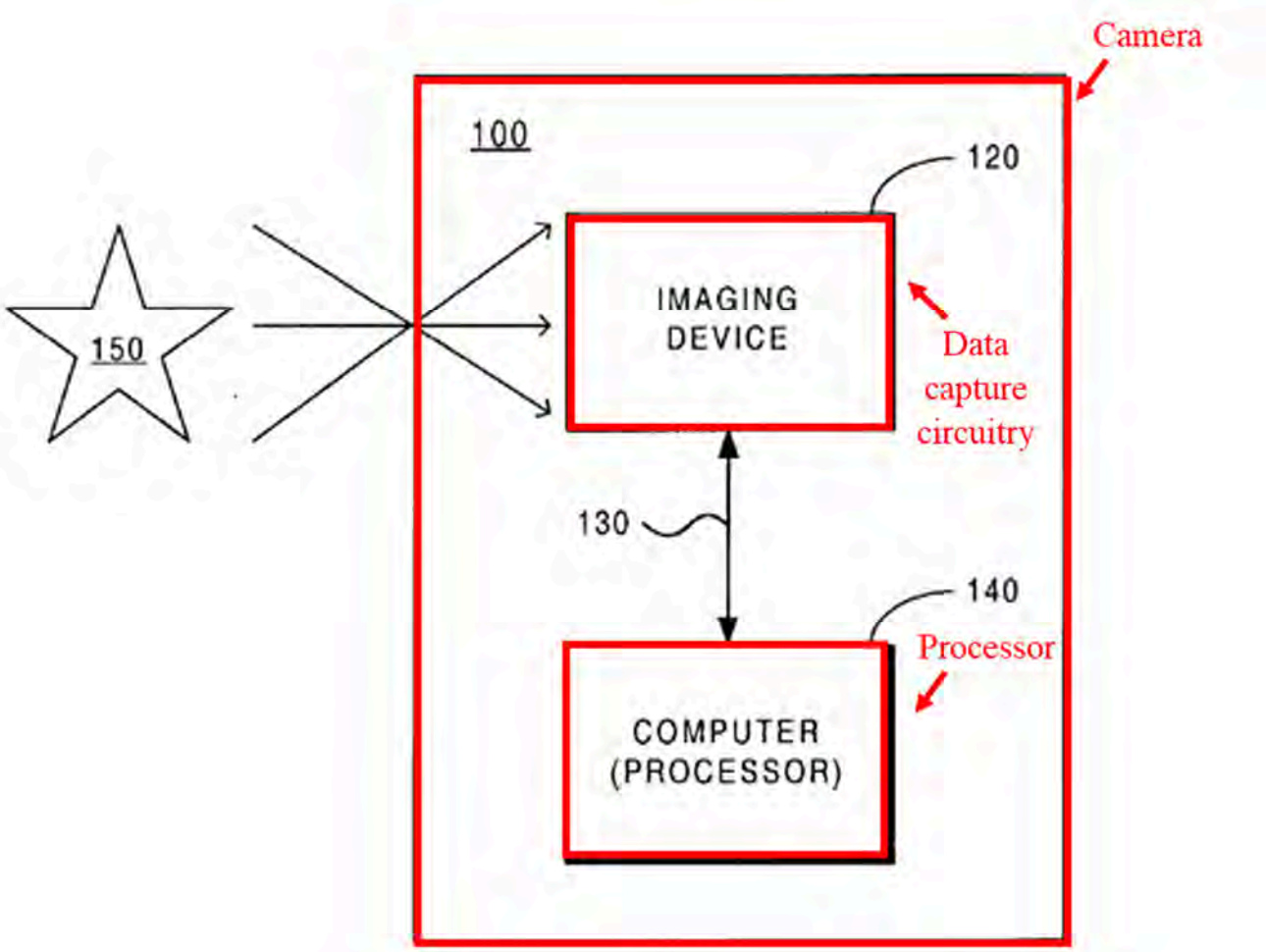


FIG. 1
(PRIOR ART)

Kahn, FIG. 1 (annotated). Kahn, [0020] ("FIG. 1 is a very general block diagram of a digital camera suitable for implementing the present invention.")

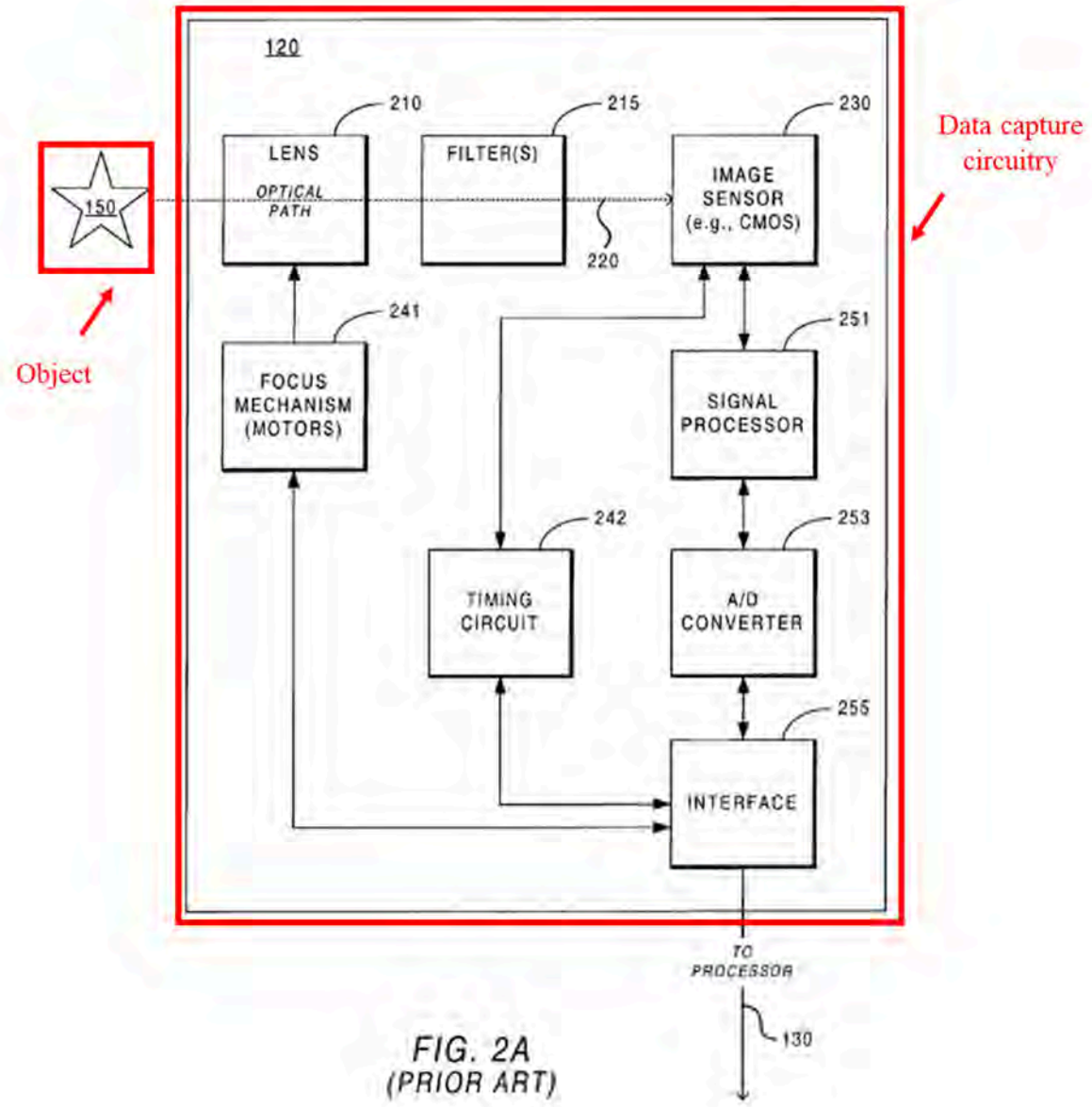


FIG. 2A
(PRIOR ART)

Kahn, FIG. 2A (annotated). Kahn, FIG. 2A (annotated). Kahn, [0021] ("FIG. 2A is a block diagram of a conventional digital imaging device.")

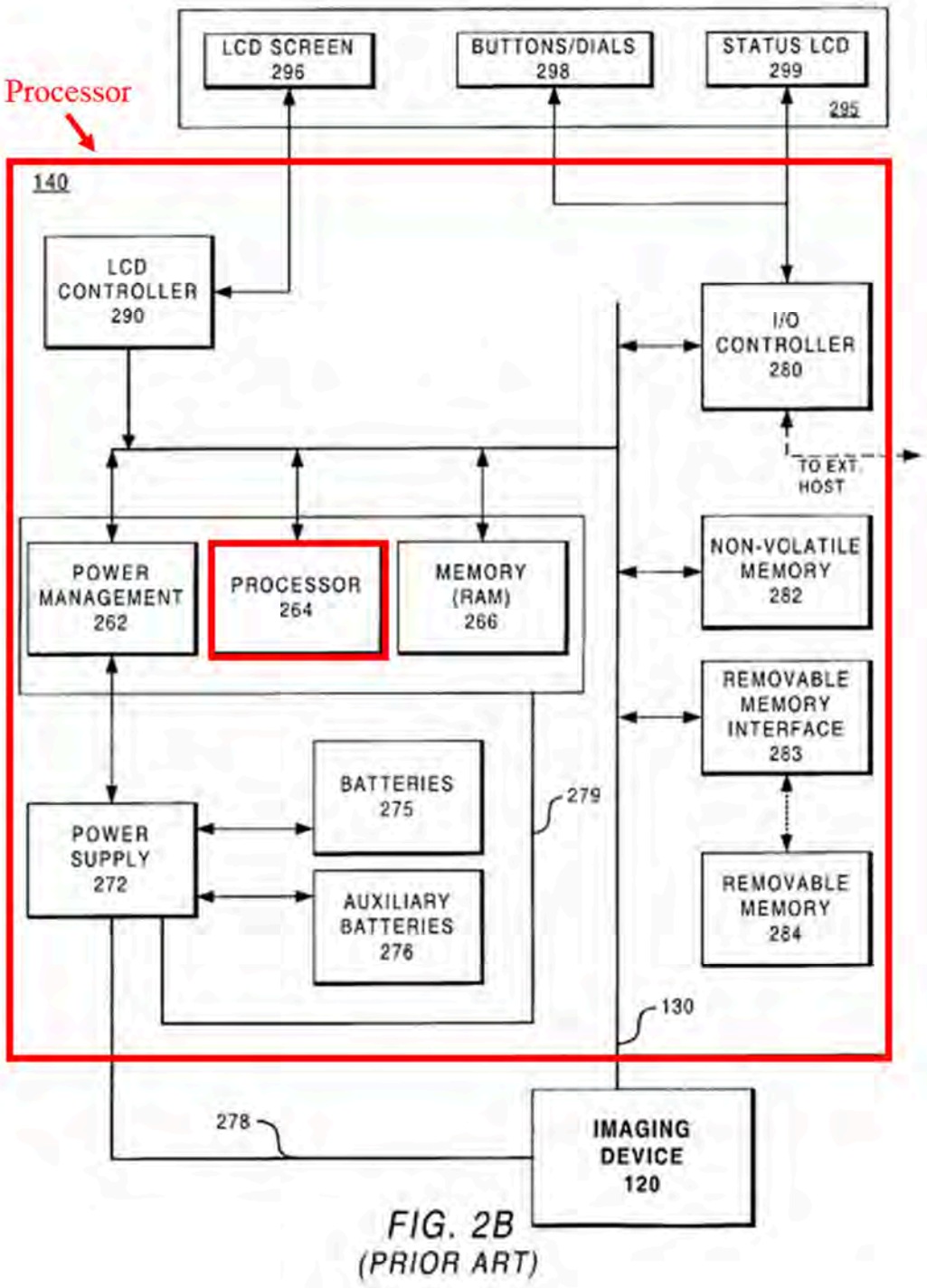


FIG. 2B
(PRIOR ART)

Kahn, FIG. 2B (annotated). Kahn, [0022] ("FIG. 2B is a block diagram of the processor or computer used for the digital imaging device of FIG. 2A.")

[1.8] wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;

715. Kahn teaches that "[t]he digital camera 100 may include the user interface 295 for providing feedback to, and receiving input from, a camera user, for example." Kahn, [0046]. Furthermore, Kahn suggests remote operation of the camera, indicating that "these [user interface] elements may be provided through a host device [cell phone] (e.g., personal digital assistant) for a media capture device implemented as a client to a host device." Id. A POSITA would have understood that Kahn teaches that a user can remotely operate camera shutter so that object 150 is "captured or recorded as a digital image, upon activation of a shutter mechanism" thus teaching that the new data is acquired after the establishing the short range wireless connection. Kahn, [0033], FIG. 1, 2A-B. See also, id., [0007].

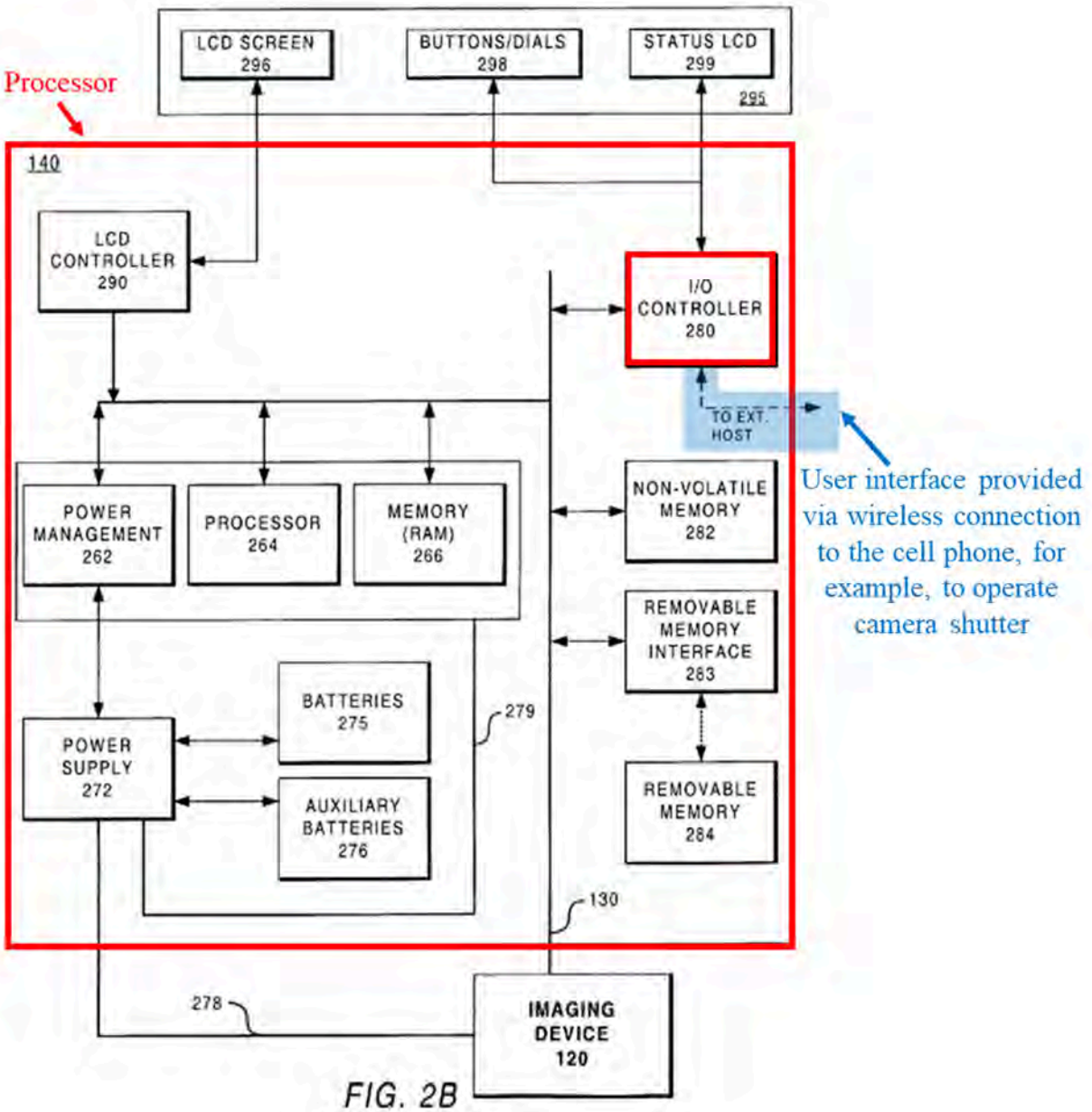


FIG. 2B
(PRIOR ART)

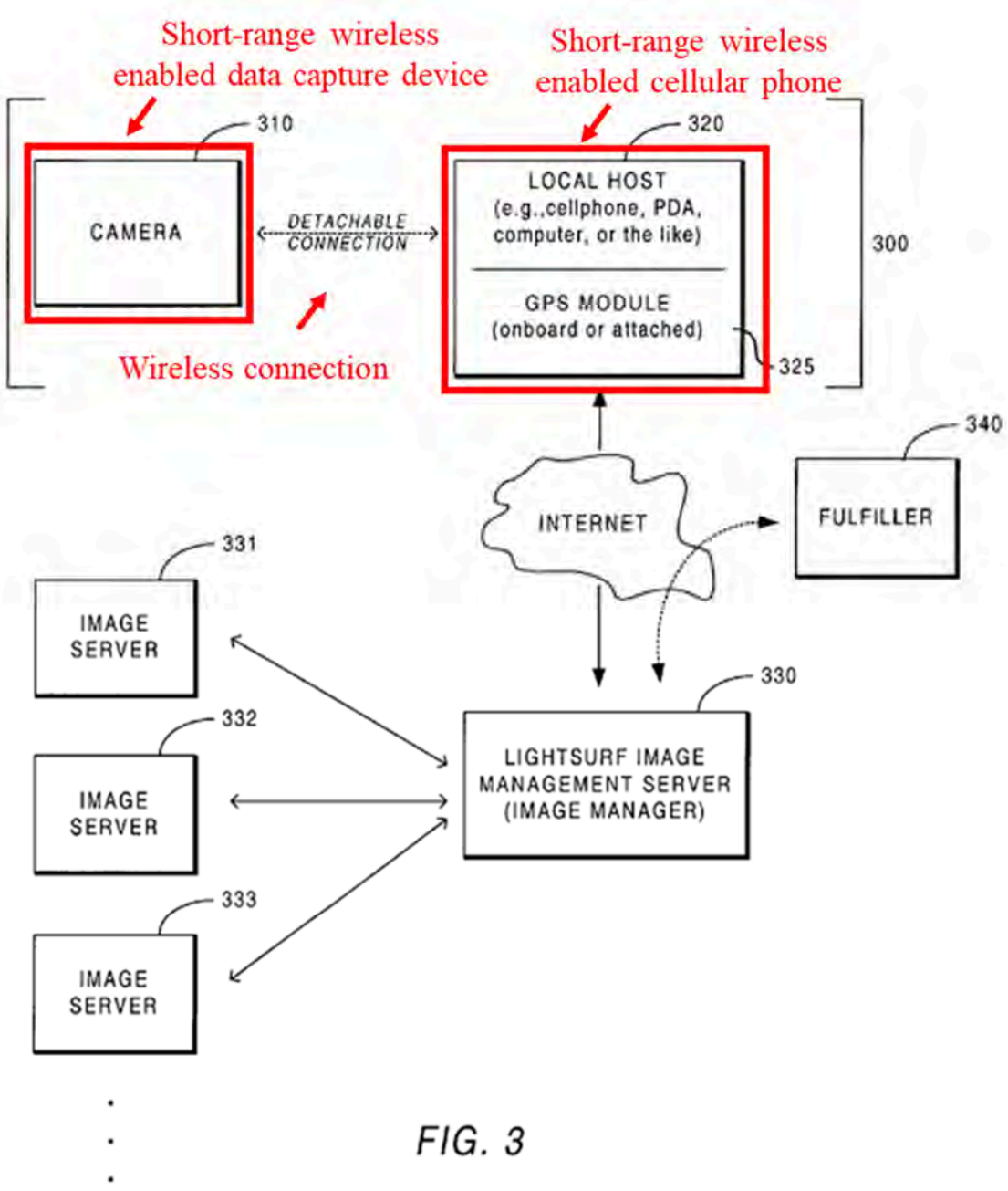


FIG. 3

Kahn, FIG. 3 (annotated). Kahn, [0023] ("FIG. 3 is a high-level block diagram illustrating the basic components that comprise the environment in which the present embodiment may be implemented.")

716. Kahn teaches "**the camera device 310 is a stand-alone unit** that is

occasionally (or **persistently) connected to the host device 320**, which may be any device capable of hosting the camera device 310. For example, host device 320 may comprise a cellular phone, a PDA (personal data assistant) with wireless connectivity, or the like. The GPS module 325 is either a stand-alone or integrated module that provides real-time GPS information to the host 320, and in turn to clients of the host (i.e., camera 310) that may submit queries for GPS information." Kahn, [0055]. Thus, a "**user employ[ing] the camera 310 to take various pictures (i.e., capture images). Immediately** or at some convenient point in time, **location ID information (i.e., GPS information) from the GPS module 325 is associated with the images that are captured**." Kahn, [0057]. A POSITA would have understood "[t]he **association of location ID information** (i.e., the GPS-derived longitude and latitude) **with one or more images [may] occur[ing] immediately (e.g., upon capture)**" is only possible because the camera is connected to the GPS-enabled cell phone when the images are being captured. Kahn, [0058], FIG. 3. Kahn specifies that the camera does not has its own GPS module so the association of the images with GPS information has to occur while the cellular phone is paired with the camera. Kahn, [0058], FIGs. 3, 4.

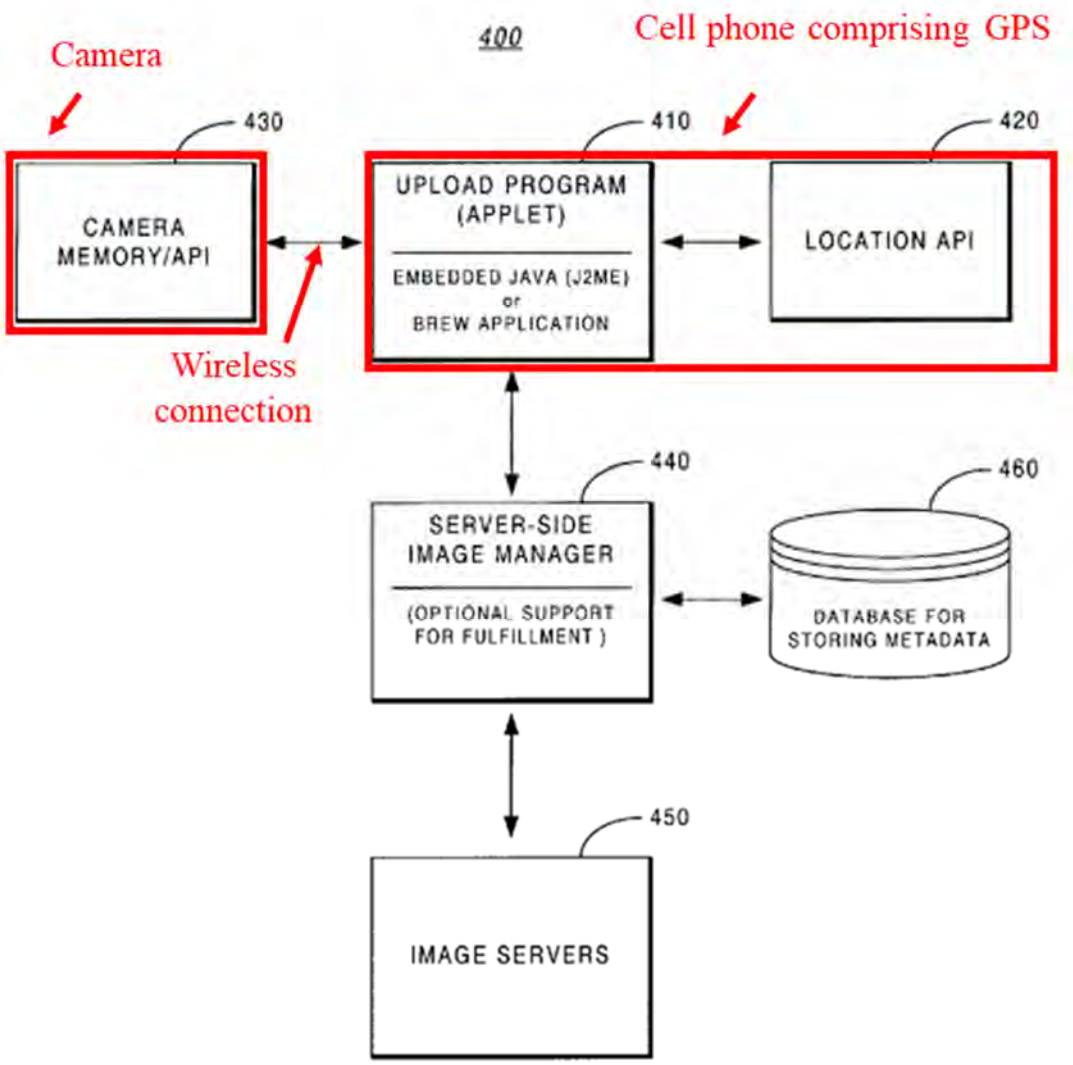


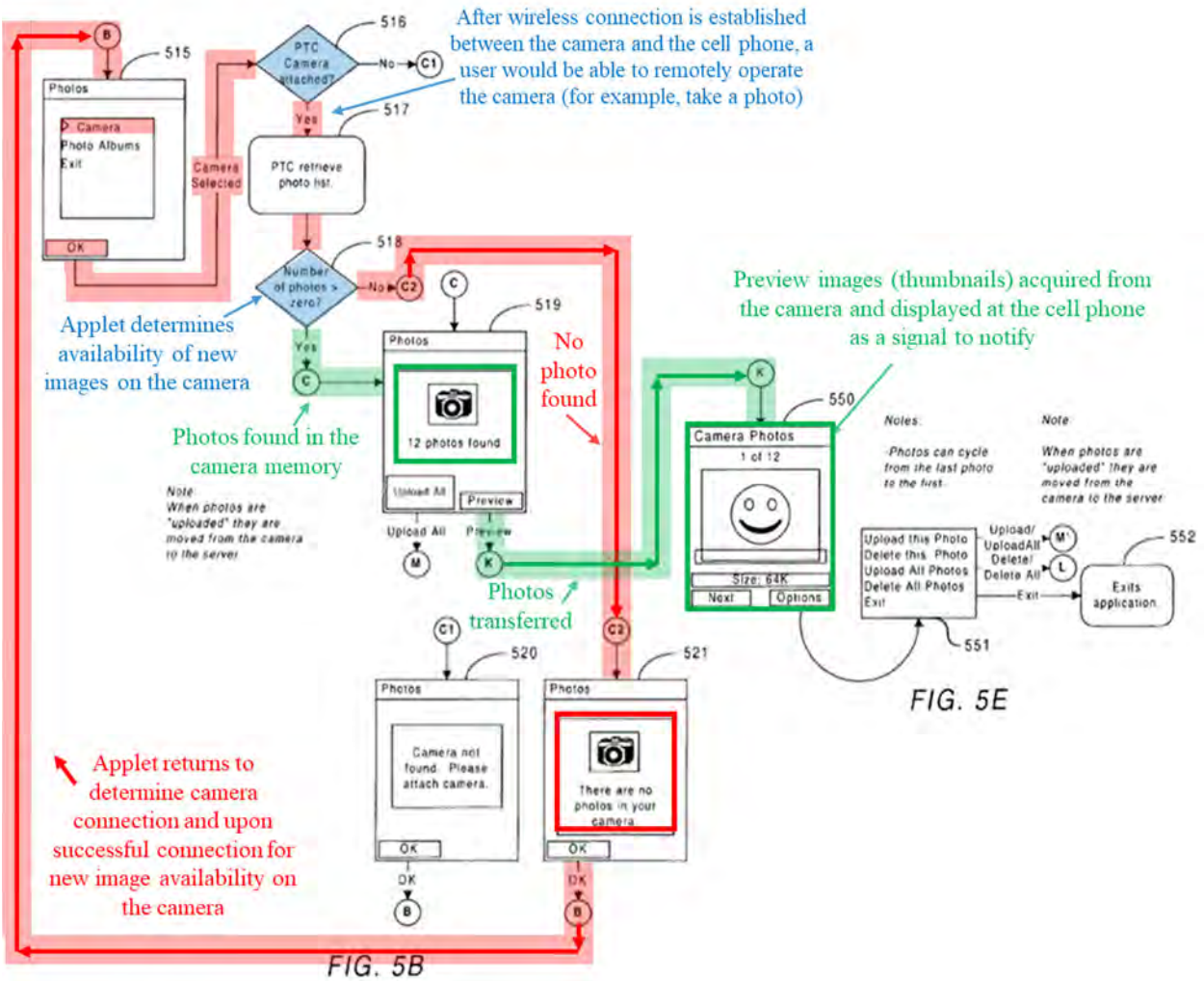
FIG. 4

Kahn, FIG. 4 (annotated). Kahn, [0024] ("FIG. 4 is a block diagram that illustrates implementation of underlying functionality (i.e., processes) in the various modules of FIG. 3.").

717. During the image capturing process, Kahn teaches "location information is automatically captured for individual photographic images

("photos")." Kahn, [0051]. Kahn also teaches that the camera performs "**association of location ID information** (i.e., the GPS-derived longitude and latitude) **with one or more images** [may] **occur[ing] immediately (e.g., upon capture)**" Kahn, [0058] (emphasis added). A POSITA would have recognized that the association of location ID information with images can only occur after the establishment of a short-range paired wireless connection between the data capture device and the cellular phone, as indicated by Kahn's description of the camera device being connected to the host device (e.g., cellular phone) for the association to take place. Kahn, [0055], FIGs. 3, 4. Kahn explicitly states that the GPS module, responsible for providing real-time GPS information to the host device and subsequently associating it with captured images, is either a stand-alone or integrated module connected to the host device, which could be a cellular phone with wireless connectivity. Id. Furthermore, Kahn's description of the upload program communicating with the camera memory/API and the location API, which returns GPS information, underscores the necessity of the camera being connected to the host device to perform the association process. Id., [0062]-[0063], FIGs. 3, 4. Therefore, a POSITA would have understood that the association of location ID information with images is contingent upon the establishment of the short-range paired wireless connection between the data capture device and the cellular phone, as taught by Kahn.

718. Kahn's "FIGS. 5A-F illustrate execution of a client-side embedded applet (i.e., a small footprint application) that executes method steps and displays exemplary user interface (UI) dialogs/menus for supporting fulfillment.", TTI-1017, [0071]. See two examples below of annotated sections of FIG. 5 that show that the phone (client side applet) continuously checks for camera connectivity. In the first example, when the number of photos is non-zero, the "Yes" between flowchart symbols 516 and 517 as part of the (red loop) shows that the phone keeps checking that the camera connection is still active.



Kahn, FIGs. 5B and 5E (partial) (annotated).

> [0074] Execution path B is employed for uploading photos from the camera. It proceeds as follows. First, the applet displays UI dialog 515, where the user is given access to photos on the camera or on photo albums (e.g., online photos), or the user may simply exit. Of interest for this example is the user selecting "Camera." 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. If the number of photos is greater than zero (tested at step 518), then the applet proceeds to execution path C (below).** If at step 516, the camera is not attached, the applet proceeds to execution path C1 (described below). If at step 518, no photos are found (i.e., the list is empty), the applet proceeds to execution path C2 (described below).
>
> [0075] Execution path C is utilized for displaying a photo uploading UI dialog 519. As shown, the UI dialog 519 indicates the number of photos found. The user may now select to "upload all" photos (execution path M, described below) or simply "preview" photos (execution path K, described below).
>
> [0079] **Execution path K is used for providing the user with an image preview, allowing individual image processing**. At execution path K, **the applet displays UI dialog 550 (FIG. 5E), which allows access to individual images on the camera**. Here, the user is given a variety of options, as indicated by dialog 551: upload this photo, delete this photo, upload all photos, delete all photos, or exit. If the user selects the option to upload the current photo or upload all photos, the applet proceeds down execution path M′. If, however, the user selects the option to delete the current photo or delete all photos, the applet proceeds to execution path L. If the user simply selected to "exit" the dialog, the applet terminates execution, as indicated by step 552.

Kahn, [0074]-[0075], [0079] (annotated).

719. Similarly, in the second example that the phone (client side applet) checks for camera connectivity is subsequent to the user's completion of uploading previously acquired photographs can be seen in flowchart symbol 544 in the annotated partial FIG 5 below, where the applet persists in its function to "determine[s] whether the camera is attached [to the cell phone]… [i]f "Yes," the list of photos is retrieved at step 545. Then, at step 546, the applet determines whether the number of photos is greater than zero. If the number is greater than zero, execution proceeds to path K." Kahn, [0086].

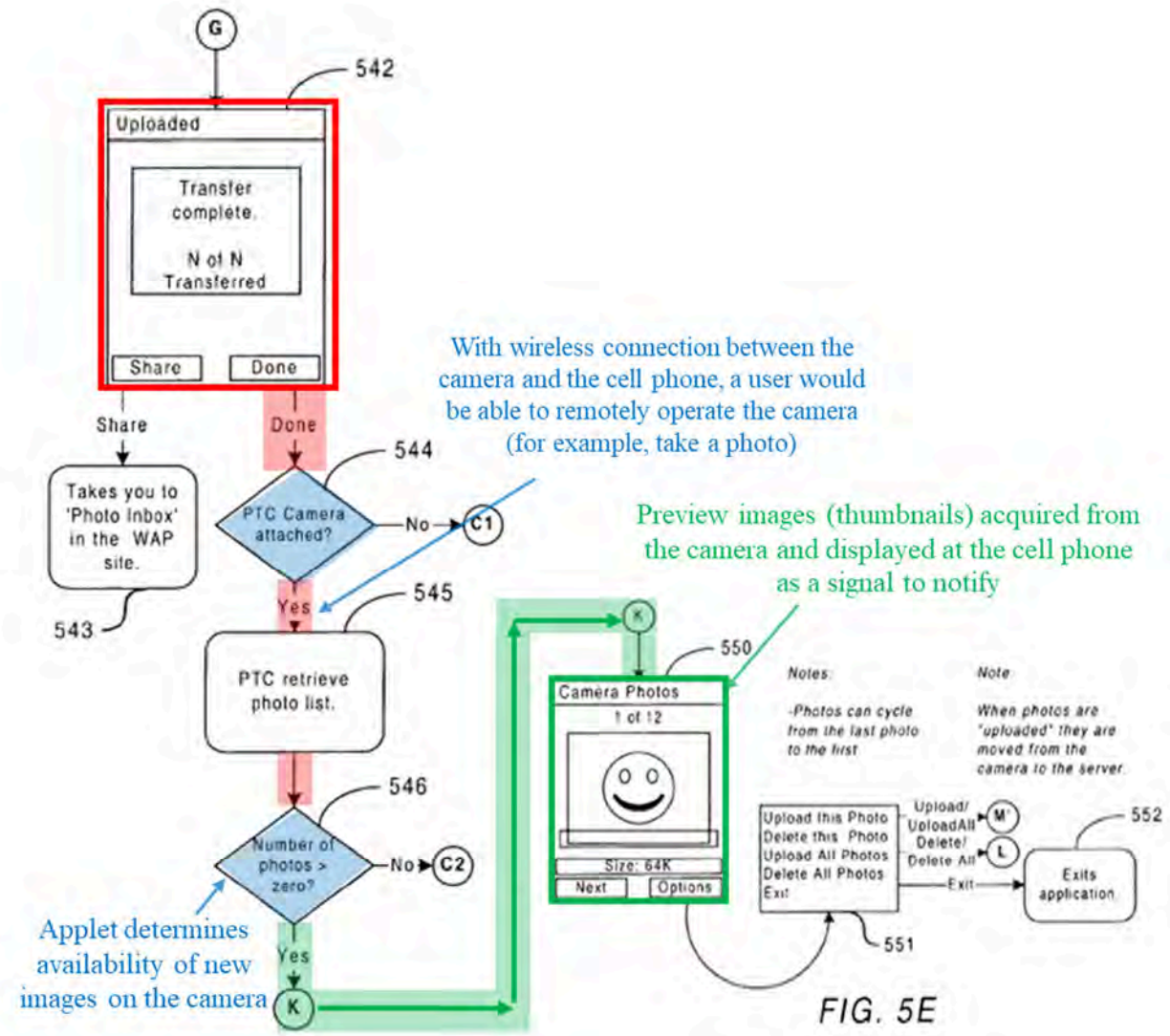


FIG. 5E

FIG. 5D

Kahn, FIGs. 5D and 5E (partial) (annotated).

[0086] Also shown in FIG. 5D, the execution path G proceeds as follows. First, an "uploaded" UI dialog 542 is displayed. Here, the user can select to "Share" the photos, or simply select "Done". In the case where the user has elected to share the photos, execution proceeds to step 543 to take the user to a "Photo Inbox" at the Web site (accessible at the local host via WAP protocol). Otherwise, in the case that the user has elected "Done", execution proceeds to step 544. **At step 544, the applet determines**

> **whether the camera is attached. If not, execution proceeds to path C1. If "Yes," the list of photos is retrieved at step 545. Then, at step 546, the applet determines whether the number of photos is greater than zero. If the number is greater than zero, execution proceeds to path K (described above).** Otherwise, execution proceeds to path C2.
>
> [0079] **Execution path K is used for providing the user with an image preview, allowing individual image processing**. At execution path K, **the applet displays UI dialog 550 (FIG. 5E), which allows access to individual images on the camera**. Here, the user is given a variety of options, as indicated by dialog 551: upload this photo, delete this photo, upload all photos, delete all photos, or exit. If the user selects the option to upload the current photo or upload all photos, the applet proceeds down execution path M′. If, however, the user selects the option to delete the current photo or delete all photos, the applet proceeds to execution path L. If the user simply selected to "exit" the dialog, the applet terminates execution, as indicated by step 552.

Kahn, [0086], [0079].

720. In the light of the Kahn's teachings, it is evident that Kahn-Feinberg-Bluetooth combination addresses the claimed limitation regarding the processor's configuration to acquire new data in the short-range wireless enabled data capture device using the data capture circuitry. Specifically, Kahn discloses a processor 140 within the digital imaging device 100, serving as the central controller, directing the operation of the imaging device and processing image data captured on it. Kahn further describes the interaction between the processor and the imaging device, where commands are issued to capture images. This aligns with

the concept of acquiring new data using data capture circuitry. Additionally, Kahn teaches remote operation of the camera via a host device, such as a cell phone, which establishes a short-range paired wireless connection, enabling the acquisition of new data after connection establishment. The disclosure illustrates the association of GPS information with captured images, indicating the acquisition of new data post-connection establishment. Kahn also teaches that the connection between the cell phone and camera are checked as part of the disclosed functionality. Therefore, a POSITA would readily recognize that Kahn teaches the processor's configuration to acquire new data through data capture circuitry after establishing a short-range paired wireless connection between the data capture device and the cellular phone.

[1.9] said processor further configured to store the new-data in the memory device;

721. The Kahn-Feinberg-Bluetooth combination renders obvious [1.9]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said processor further configured to store the new-data in the memory device. For example, Kahn teaches "captured image data is transferred over the system bus 130 to the computer 140 which performs various image processing functions on the image data before storing it in its internal memory." Kahn, [0035].

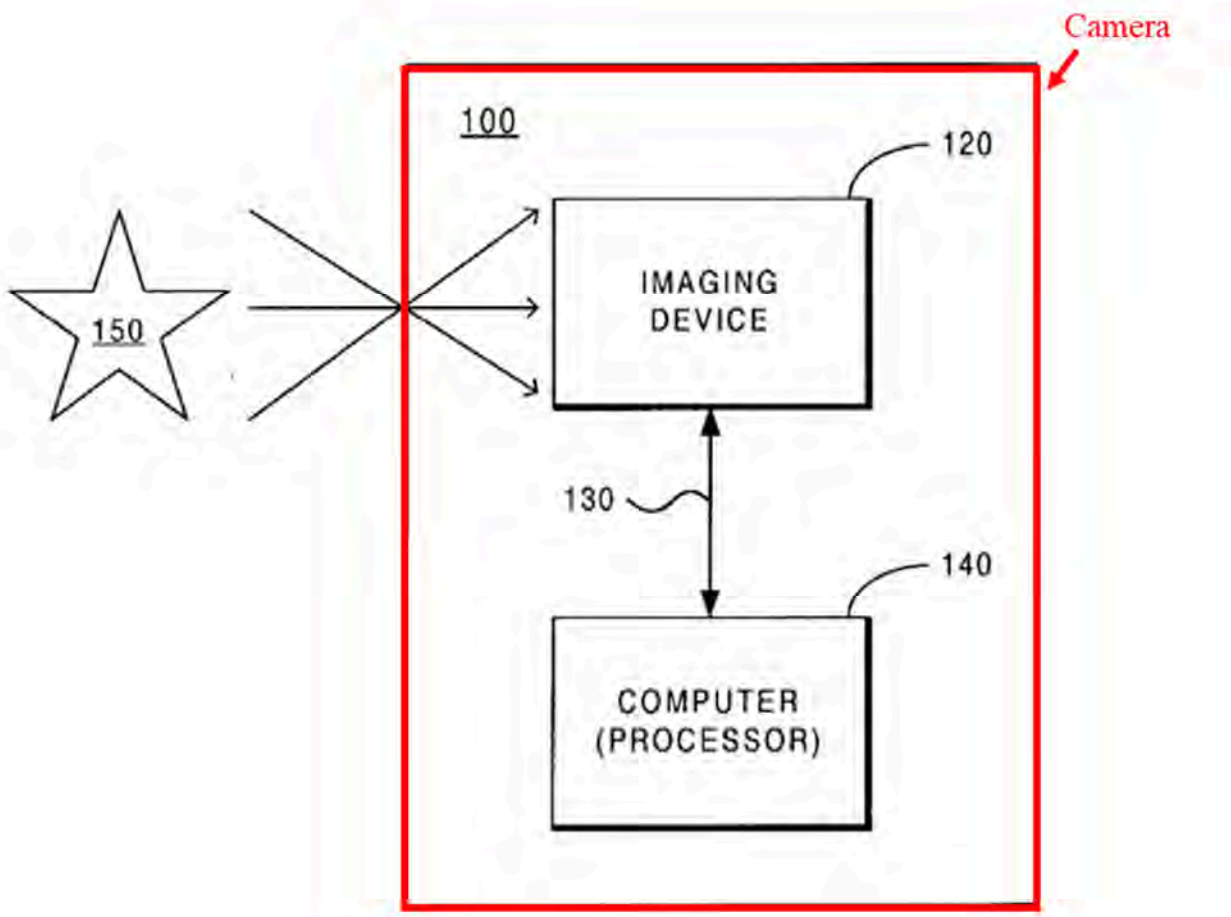


FIG. 1
(PRIOR ART)

Kahn, FIG. 1 (annotated). Kahn, [0020] ("FIG. 1 is a very general block diagram of a digital camera suitable for implementing the present invention.").

722. In FIG. 2B, Kahn illustrates "[a] conventional onboard processor or computer 140 is provided for directing the operation of the digital camera 100 and processing image data captured on the imaging device 120. FIG. 2B is a block diagram of the processor or computer 140. As shown, the system bus 130 provides

connection paths between the imaging device 120, an (optional) power management 262, a processor (CPU) 264, **a random-access memory (RAM) 266**, an input/output (I/O) controller 280, **a non-volatile memory 282, a removable memory interface 283**, and a liquid crystal display (LCD) controller 290. **Removable memory 284** connects to the system bus 130 via the removable memory interface 283. Alternately, the camera 100 (and therefore the onboard computer 140) may be implemented without the removable memory 284 or the removable memory interface 283." Kahn, [0042].

723. Further, Kahn discloses that "[t]e digital camera 100 includes several memory components. **The memory (RAM) 266 is a contiguous block of dynamic memory that may be selectively allocated to various storage functions.** Dynamic random-access memory is available from a variety of vendors, including, for instance, Toshiba of Japan, Micron Technology of Boise, Id., Hitachi of Japan, and Samsung Electronics of South Korea. **The non-volatile memory 282, which may typically comprise a conventional read-only memory or flash memory, stores a set of computer-readable program instructions to control the operation of the camera 100. The removable memory 284 serves as an additional image data storage area and may include a non-volatile device, readily removable and replaceable by a camera 100 user via the removable memory interface 283.** Thus, a user who possesses several removable memories

284 may replace a full removable memory 284 with an empty removable memory 284 to effectively expand the picture-taking capacity of the camera 100. The removable memory 284 is typically implemented using a flash disk. Available vendors for flash memory include, for example, SanDisk Corporation of Sunnyvale, Calif. and Sony of Japan. Those skilled in the art will appreciate that the digital camera 100 may incorporate other memory configurations and designs that readily accommodate the image capture and processing methodology of the present invention." Kahn, [0044].

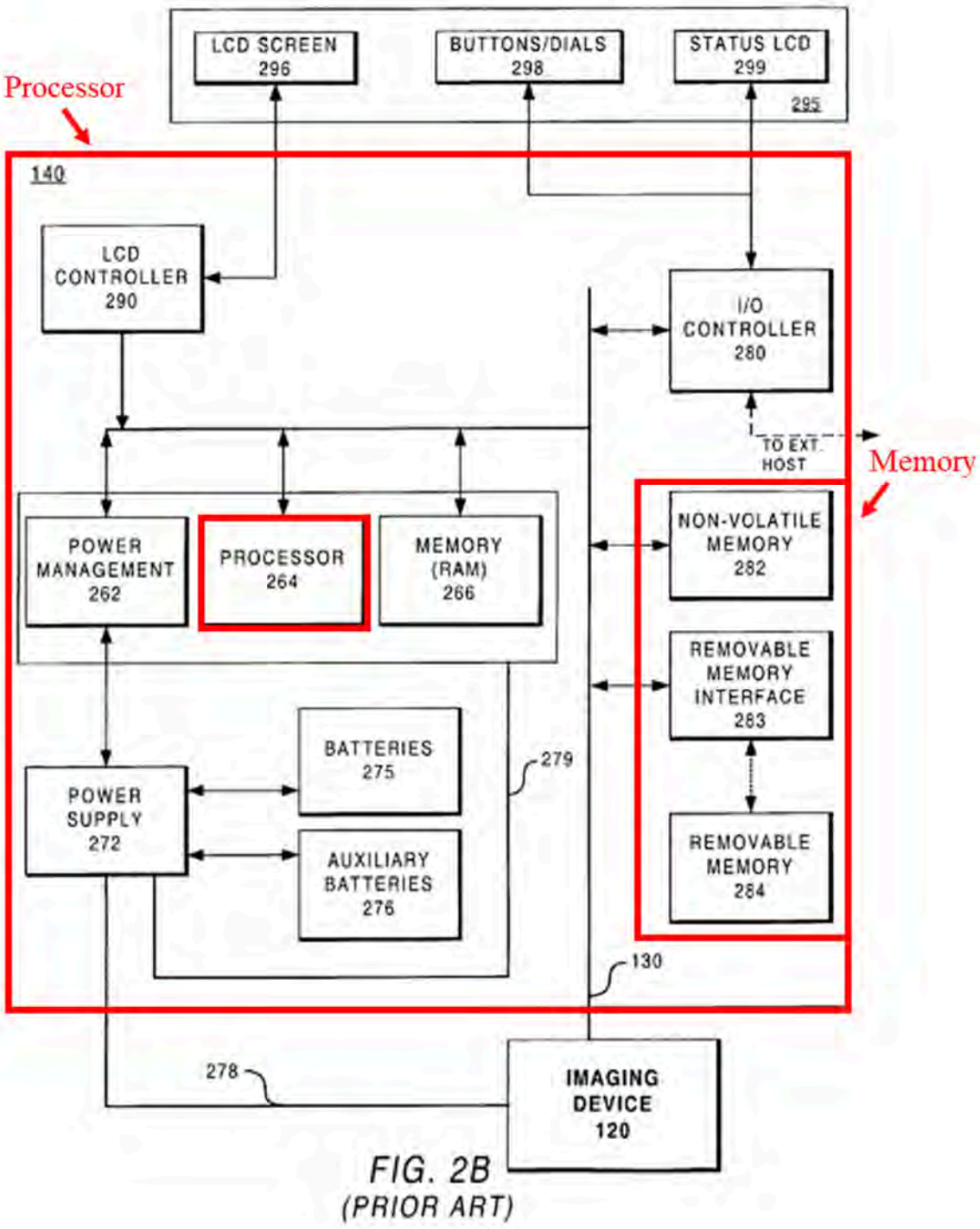


FIG. 2B
(PRIOR ART)

Kahn, FIG. 2B (annotated). Kahn, [0022] ("FIG. 2B is a block diagram of the processor or computer used for the digital imaging device of FIG. 2A.")

724. Kahn discloses a "system 300 [that] includes **a camera device 310**, a

host device 320, and a GPS (Global Positioning System) module 325. **The camera device 310 is preferably a wireless camera device**, **such as camera device 100 (shown in FIG. 1A)**, that either includes wireless connectivity itself or connects to a local host with wireless connectivity." Kahn, [0055], FIGs. 1A, 3.

725. A POSITA would have understood that the processor 254 in the camera device 310 (or camera device 100) will be configured to store captured image data (new-data) in its internal memory (for example, a non-volatile memory 282, a removable memory interface 283, and removable memory 284). Kahn, [0035], [0042].

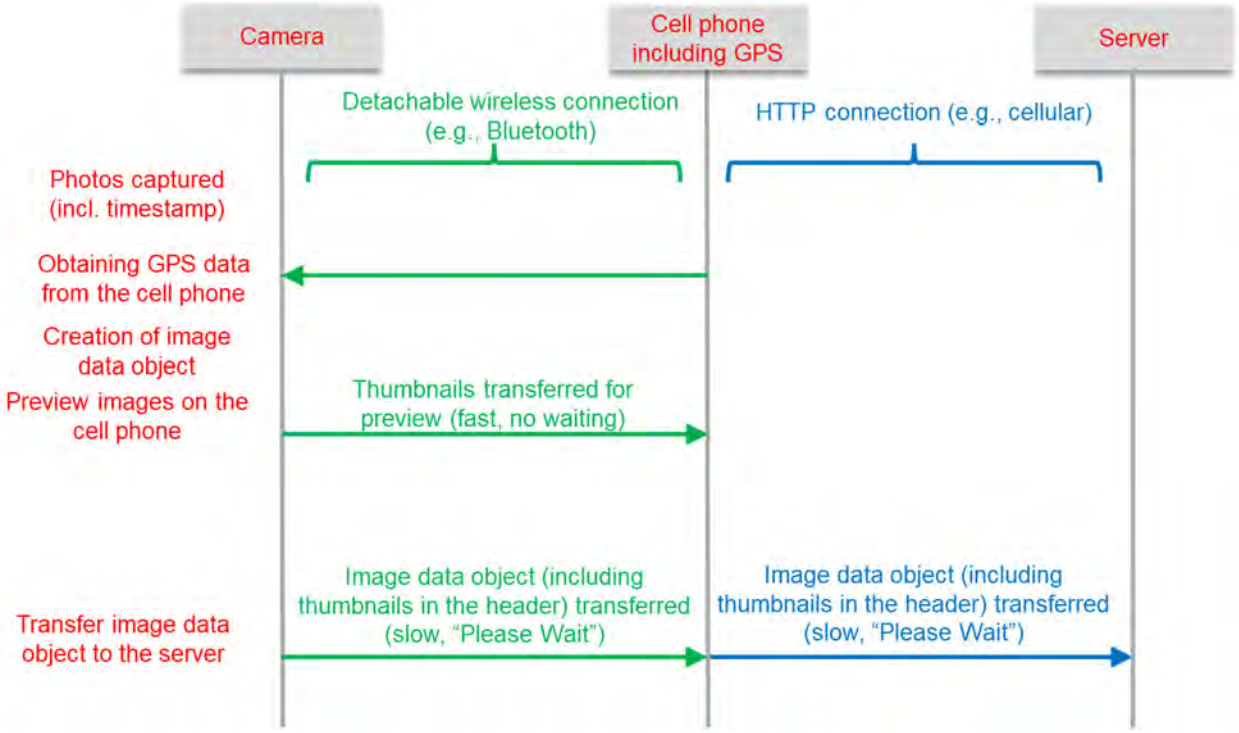
[1.10] said processor further configured to create a new-data object, wherein the new-data object comprises:

726. The Kahn-Feinberg-Bluetooth combination renders obvious [1.10]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said processor further configured to create a new-data object.

727. As discussed above (supra [1.7]-[1.8]), Kahn teaches capturing photos (acquiring new-data), for example in step 701 of FIG. 7. During the image capturing process, Kahn also teaches acquiring associated new data such as GPS location information and time stamp information and that "location information is automatically captured for individual photographic images ('photos')."", Kahn, [0058], [0008], [0098]. Kahn also teaches acquiring Thumbnails of full image data as signal to notify of acquisition of the corresponding new full image data,

"UI dialog 519 indicates the number of photos found.", Kahn, [0075], FIG. 5B.

728. See an illustration I made below for the following discussion that shows the high level flow of the data object including the timestamp, full resolution image, and thumbnails.



729. Kahn shows that the thumbnails can be previewed in screen 550 and there is no wait time shown after selecting preview., Kahn, FIG. 5E. Kahn teaches that "When photos are 'uploaded', they are moved from the camera to the server." via the cellular phone, Kahn, FIGs. 5B, 5E, [0063]. Because Kahn shows in step 550 of FIG 5E, before uploading the full resolution image to the phone that the thumbnails can be previewed on the phone, a POSITA would understand the thumbnails are stored (at least temporarily for buffering) on the camera along with

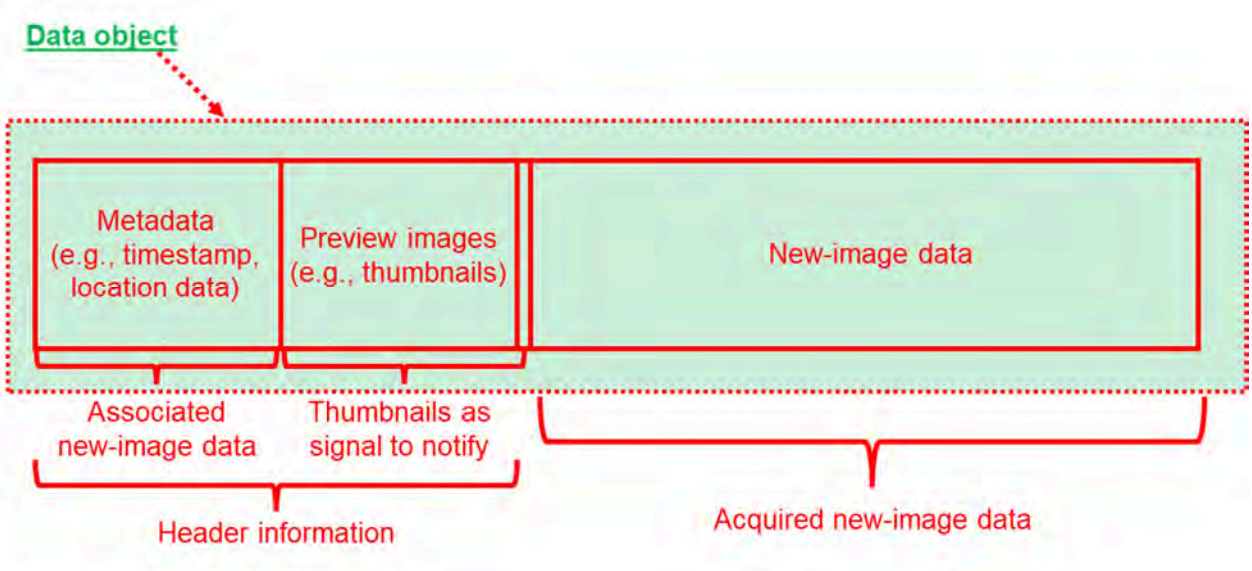
the full resolution images as part of the data object. Kahn shows in FIG. 5C that when uploading each data object from the camera to the server including the full resolution images, it takes long enough time that a "Please wait" message is shown in screen 528 on the phone., Kahn, FIG. 5C. A POSITA would understand that because there is no wait time for previewing thumbnails on the phone as compared to wait time for uploading images to mean that the only thumbnails are transferred from the camera to the phone during preview. Feinberg teaches that the uploaded "thumbnail images (e.g., having 160×120 pixel resolution) are typically embedded into the full resolution image file header.", Feinberg, [0091].

730. Furthermore, the GPS location information and timestamp are stored on the phone and uploaded with the thumbnails and full image data. Kahn teaches that metadata associated with the image is being stored in the header of its corresponding image, for example, "the location ID information may be stored together with the image data that comprises the image (e.g., stored in a header)." Kahn, [0059]. Also, Kahn teaches the camera performs "**association of location ID information** (i.e., the GPS-derived longitude and latitude) **with one or more images** [may] **occur[ing] immediately (e.g., upon capture)**" Kahn, [0058]. In addition to GPS information, Kahn also teaches associating timestamp with the image captured. Kahn, [0060] ("the image data already includes timestamp information (i.e., timestamp indicating when the image is captured)"). See also,

Kahn, [0008] and [0098].

731. A POSITA would thus understand that the thumbnails, full resolution images, and metadata (timestamp, location information) are stored on the camera and uploaded to the server through the phone as a data object. Kahn teaches that "[t]he upload program 410 assembles the image data for the images and the corresponding metadata comprising location information and user (identity) information, and then transmits all of that information/data [from the camera to the cell phone and then] to the image management server, via its communication with the server-side application 440 .", [0064]

732. See an illustration below that I made of a new-data object prepared based on the teachings of Kahn-Feinberg combination.



733. A POSITA would have recognized that the said processor, as described by Kahn, is further configured to create a new-data object based on the

captured images and associated location ID information. Kahn, [0051], [0058], [0064]-[0065], [0098]. Kahn's disclosure of the camera device's functionality includes not only capturing photos but also "automatically" associating them with GPS-derived location information immediately upon capture. Id. This association process involves the processor within the camera device, which directs the operation of the imaging device and facilitates the processing of image data. Id., [0034]. Moreover, Kahn's explanation of the upload program's interaction with the camera memory/API and the location API, which returns GPS information, highlights the involvement of the processor in creating a new-data object by associating images with location data. Id.,[0051], [0062]-[0063], FIGs. 3, 4. Since this association occurs as part of the image capturing process facilitated by the processor, a POSITA would have readily recognized that the processor would have been further configured to create a new-data object comprising images (new-data) associated with location information (associated new-data), as taught by Kahn.

734. A POSITA would have understood that creating a new-data object would include creating preview images (i.e. thumbnails) as disclosed in Kahn. Kahn, [0075] ("simply "preview" photos"), [0079] ("Execution path K is used for providing the user with an image preview, allowing individual image processing. At execution path K, the applet displays UI dialog 550 (FIG. 5E), which allows access to individual images on the camera."), FIG. 5E (figure element 550), FIG. 6

(thumbnails related to albums shown in figure element 601).

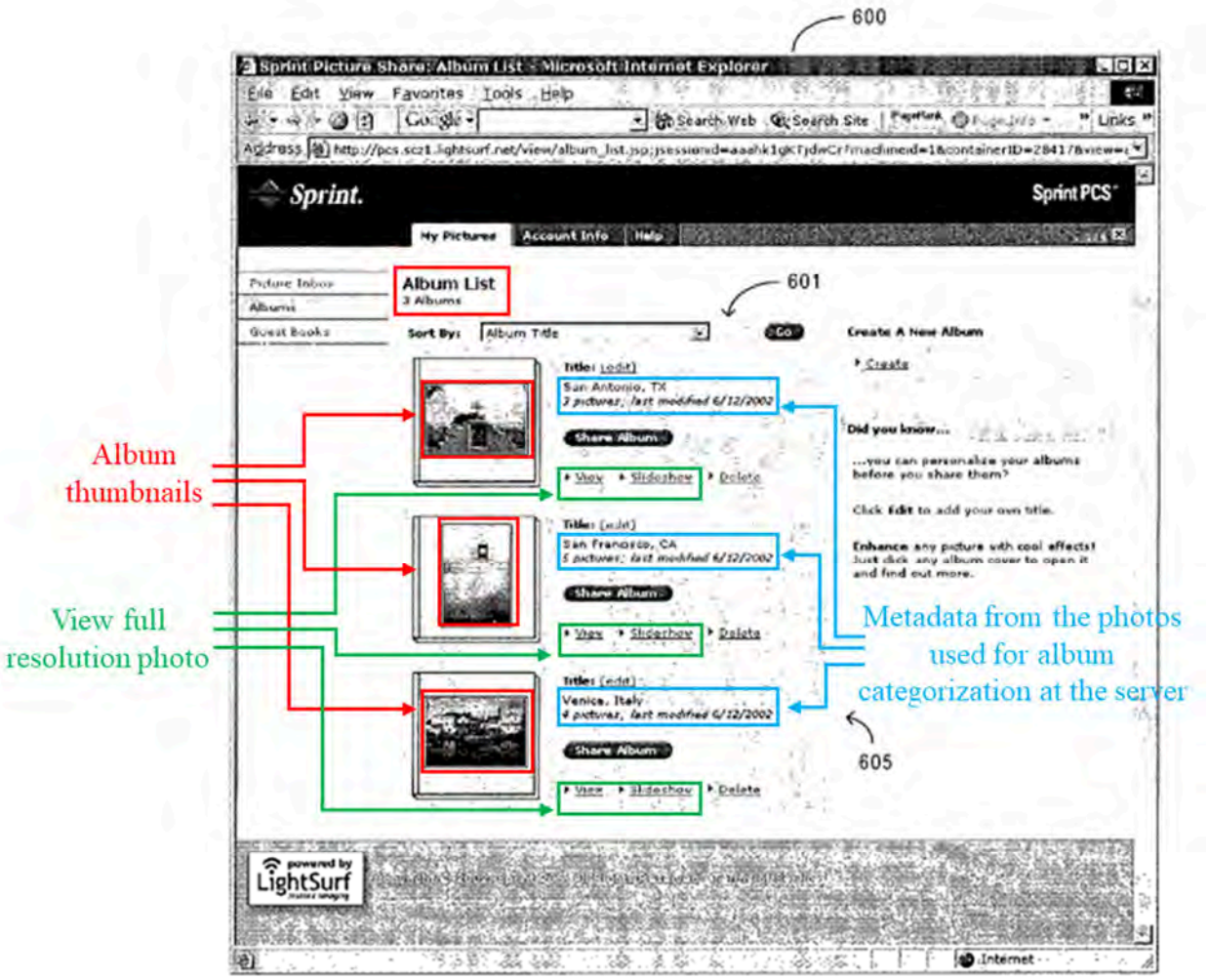


FIG. 6

Kahn, FIG. 6 (annotated). In FIG. 6, Kahn illustrates, thumbnails being displayed on a "a browser-based interface for accessing one's photos on-line." Kahn, [0027], [0089].

735. A POSITA would have been motivated to implement the teaching of Feinberg so that the thumbnail images are "typically embedded into the full

resolution image file header." Feinberg, [0091]. The inclusion of thumbnails in the header would require any additional image processing as Feinberg teaches that "thumbnails are extracted from the image files and transmitted, with no additional image processing." Id.

736. Kahn also teaches that "the image data already includes timestamp information (i.e., timestamp indicating when the image is captured)." Kahn, [0060]. Thus, POSITA would have understood that creation of the new-data object would include the associated metadata of the image as part of the header. Kahn, [0058]-[0059].

737. First, the creation process serves the purpose of transmitting data from one device to another. As discussed above, the creation of thumbnails facilitates the transmission of image data from the digital camera to the mobile phone which is analogous to the creation of a new-data object (generation of data) that needs to be transmitted.

738. Second, a POSITA would have understood that the thumbnails themselves serve as the signal representing the event notification, indicating to the mobile phone that new data is available. In light of the disclosure presented in Kahn, a POSITA would have understood that creating a new-data object shares conceptual similarities with the creation of preview images (i.e. thumbnails) and the metadata stored together with the image data serving as mechanisms for

transmitting data between devices and signaling events or the availability of new data. Kahn, [0058]-[0059], [0062], [0064]-[0065], [0098]; Feinberg, [0091].

[1.11] 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;

739. The Kahn-Feinberg-Bluetooth combination renders obvious [1.11]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests 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.

740. As discussed above (supra [1.10]), a POSITA would have understood that creating thumbnails in Kahn would constitute as a signal to notify particularly, for transferring new data to the mobile phone from camera, for example as shown in the phone screen 519. Kahn, [0075], FIG. 5B. See also Supra [1.3].

[1.12] the acquired new-data; and

741. The Kahn-Feinberg-Bluetooth combination renders obvious [1.12]. As discussed above (supra [1.10]), in my opinion, Kahn-Feinberg-Bluetooth teaches or suggests the acquired new-data.

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

742. The Kahn-Feinberg-Bluetooth combination renders obvious [1.1]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests associated new-data, wherein the associated new-data corresponds to data associated with the new-data.

See Supra [1.10] with the associated new data being at least the location information and the timestamp.

For example, Kahn discloses "automatically" forming metadata associated (associated new-data) with each captured image data. Kahn, [0051], [0062], [0065]. Kahn states that in prior art "imaging devices have only been able to record information about the date/time (timestamp) that an image was captured but not information about the location where the image was captured." Kahn, [0008]. During the uploading process, "[t]he upload program 410 assembles the image data for the images and the corresponding metadata comprising location information and user (identity) information" Kahn, [0064]. "The metadata … includes fields for user ID, timestamp (date/time), and location ID (longitude and latitude decimal values). Kahn, [0098].

[1.14] 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,

743. The Kahn-Feinberg-Bluetooth combination renders obvious [1.14]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests 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. For example, Kahn discloses that "[t]he

upload program 410 is implemented as an embedded application in the camera device, the host device, or a combination thereof. …[t]**he upload program 410 is invoked, automatically** … to upload images to the user's account on an image server." Kahn, [0062]. "[T]he upload program 410 also communicates with the camera memory/API 430 , so that the upload program 410 can retrieve images from the camera [internal memory of camera]. In this manner, the upload program 410 is able to invoke [automatic] transfer of the images from the camera to the host (e.g., cell phone), for uploading to a destination image server." Kahn, [0063]. See also, Kahn, [0069].

744. In FIG. 7, Kahn illustrates "a high-level flowchart summarizing a method 700 of operation of the present invention for the automated uploading and organizing of photographic images, based on location information.", "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. At step 703, upon receipt of the request that the images be uploaded, a local application (applet) is invoked that associates location information with the images…Next, the applet transmits this location ID to the image manager, as part of the transmission that

uploads the images." Kahn, [0097].

745. Kahn teaches that the new data object goes from the camera, to the cell phone, and then to the server. As shown in FIG. 5D, Kahn illustrates automatic "transfer of the images from the camera to the host (e.g., cell phone), for uploading to a destination image server.", Kahn, [0063]. Kahn specifies automatic transfer using Execution path HI, outlined in FIG. 5D, which entails several sequential actions. Kahn, [0085]. Initially, at step 536, the applet initiates a media transfer by sending a corresponding message. Kahn, [0085]. Subsequently, at step 537, the applet verifies the presence of a valid data connection. If such a connection exists, the execution progresses to step 538, where the applet proceeds to process a media transfer acknowledgment message. Kahn, [0085]. However, in the event of an unsuccessful acknowledgment (step 539), execution diverts to path F, directing to dialog 531. Kahn, [0085]. Conversely, upon a successful acknowledgment, the applet proceeds to step 540, wherein it deletes the photo from local storage. Kahn, [0085]. Following this, at step 541, the applet evaluates whether additional photos necessitate transfer. If affirmative, the execution loops back to step 536 to commence the process anew. Kahn, [0085].

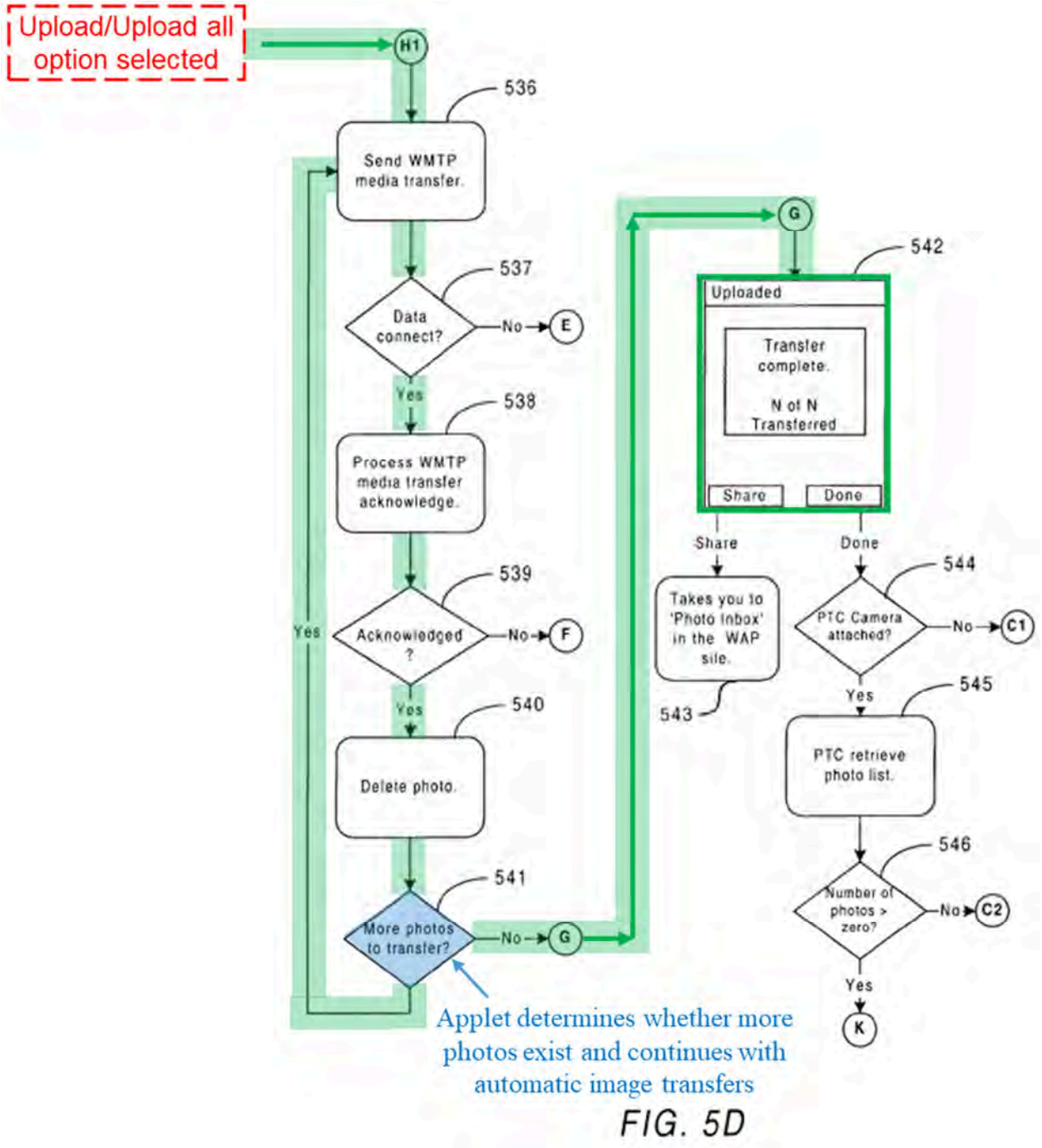
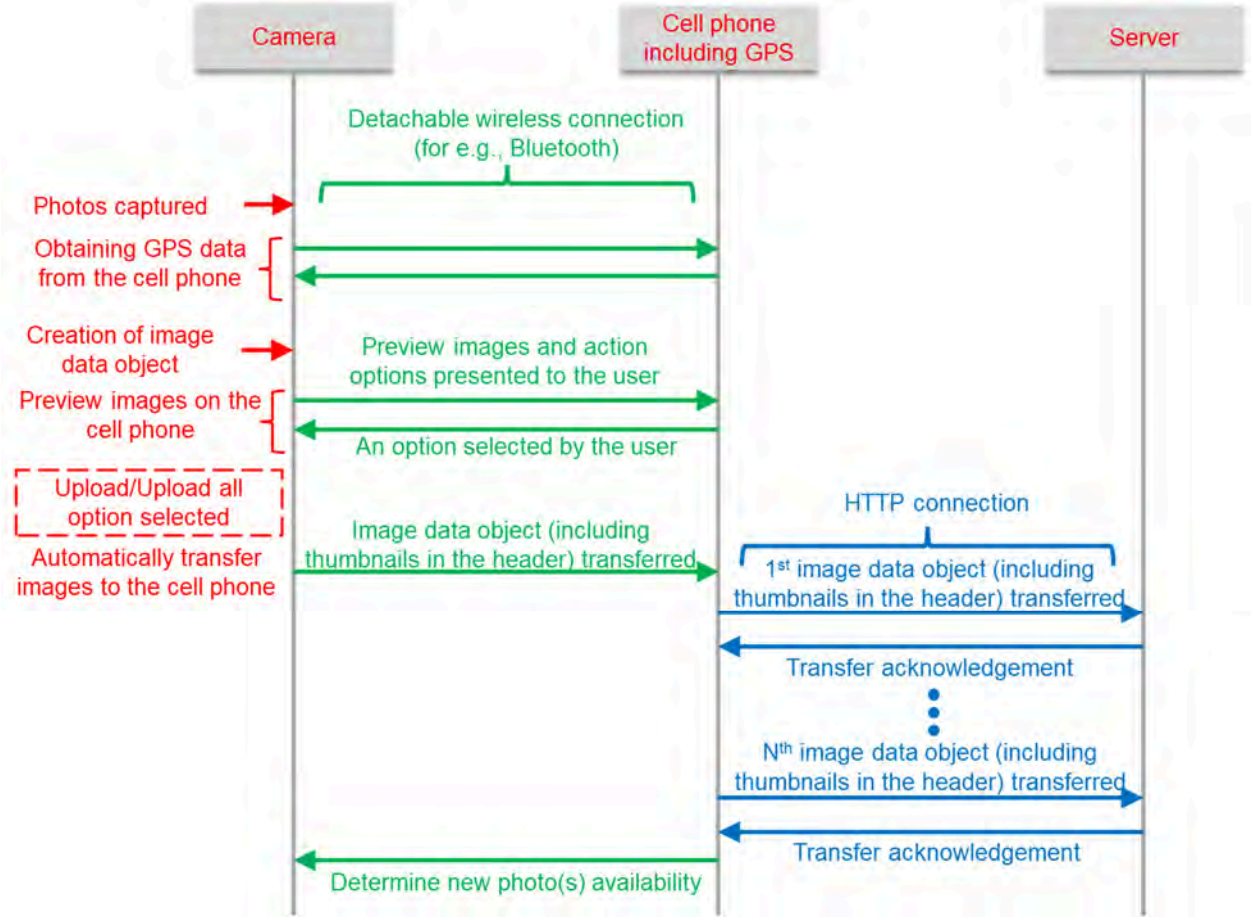


FIG. 5D

Kahn, FIG. 5D (annotated)

746. See the illustration I made below showing the flow of the data object.



[1.15] 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,

747. The Kahn-Feinberg-Bluetooth combination renders obvious [1.15]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests 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. Supra [1.10]. For example, Kahn discloses "the 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." Kahn, [0057]. Kahn discloses that in cell phone's graphical user interface (GUI) that 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. If the number of photos is greater than zero (tested at step 518)" Kahn, [0074], FIG. 5B.

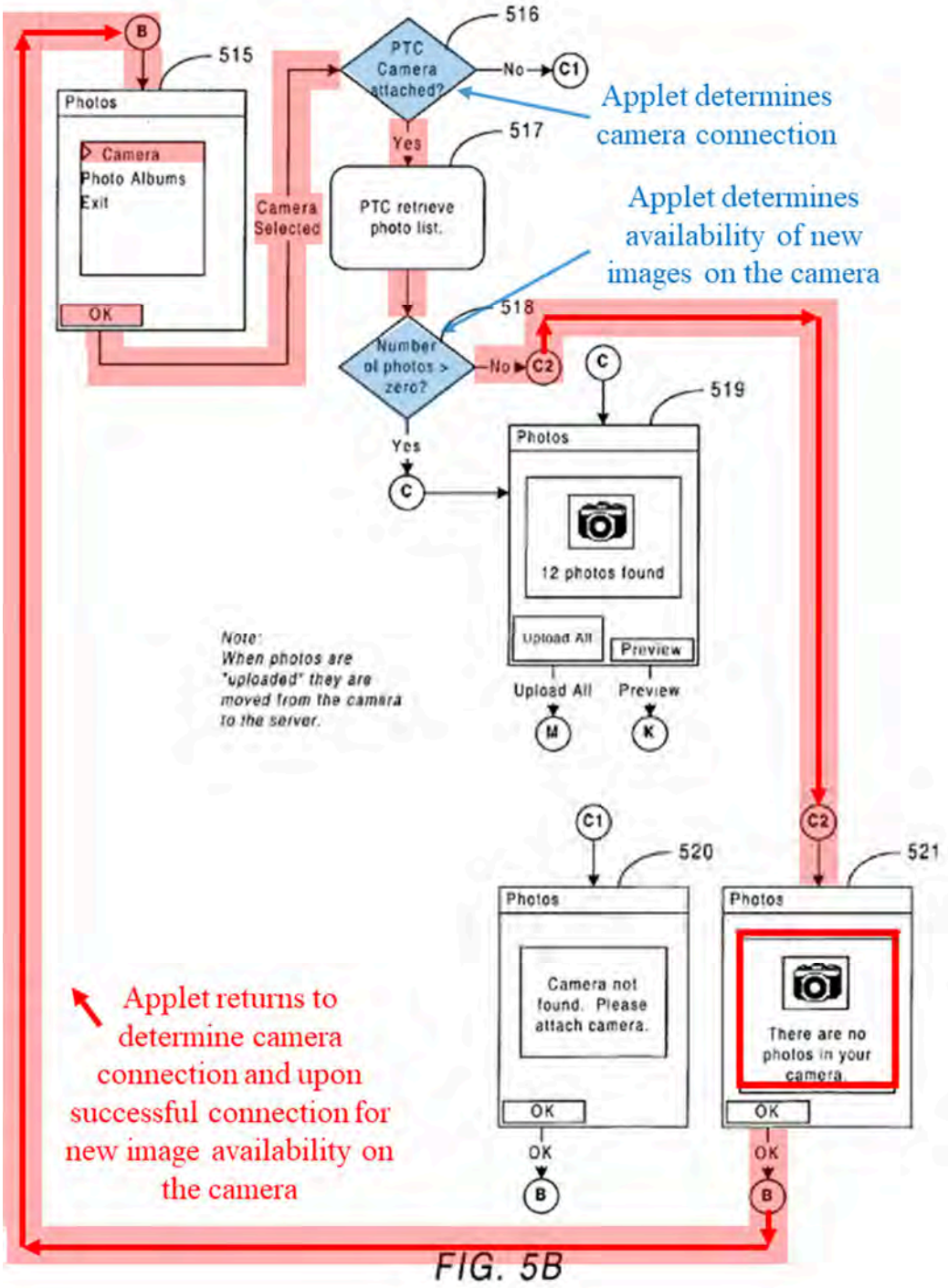


FIG. 5B

Kahn, FIG. 5B (annotated). A POSITA would have recognized that cell phone determining number of photos available on a camera would constitute as listening. Kahn, [0074], [0076], FIG. 5B.

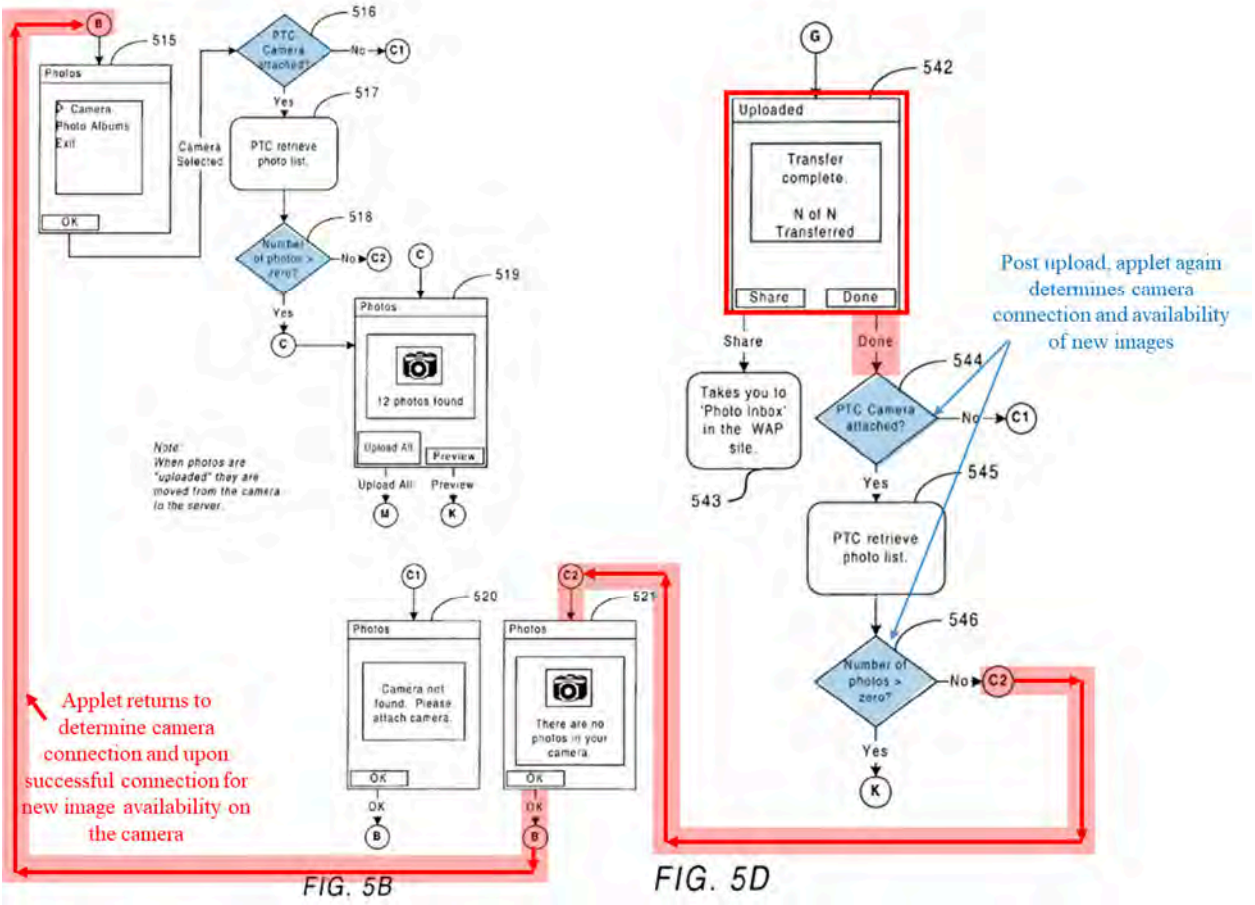


FIG. 5B FIG. 5D

Kahn, FIG. 5B and 5D (partial) (annotated). Post uploading of photos to the server (refer figure element 546 in FIG. 5D), Kahn teaches that the cell phone once again determines number of photos available on a camera would constitute as listening. Kahn, [0074], [0076], FIG. 5B. As discussed above (supra [1.10] and [1.12]), Kahn discloses cell phone configured to receive new-data object.

[1.16] wherein a mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the signal to notify and store the received new-data in a memory device of the cryptographically authenticated short-range wireless enabled cellular phone,

748. The Kahn-Feinberg-Bluetooth combination renders obvious [1.16]. In

my opinion, Kahn-Feinberg-Bluetooth teaches or suggests wherein a mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the signal to notify and store the received new-data in a memory device of the cryptographically authenticated short-range wireless enabled cellular phone.

This limitation is broken down into constituent steps below:

[1.16.1] wherein a mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the signal to notify

749. As discussed above (supra [1.3]), Kahn teaches that the camera 310 is wirelessly connected with the local host 320 (for example, a cell phone) . Kahn, [0055], FIG. 3. Kahn teaches "the client-side applet program, which may be embodied as an embedded J2ME applet in the local host" for example a cell phone. Kahn, [0071], [0055]. Kahn teaches that "a client-side embedded applet (i.e., a small footprint application) [that] executes method steps and displays exemplary user interface (UI) dialogs/menus for supporting fulfillment." Kahn, [0071]. Accordingly, the applet performs different functions, for example, "applet determines whether the camera is currently connected to the local host [for e.g., cell phone]", "applet determines whether the number of photos is greater than zero", "applet displays UI menu," "applet establishes a connection to the photo site (Web-based server providing image management) for uploading of photos." Kahn,

[0070]-[0086], FIGs. 5A-5F.

750. As discussed above (supra [1.10]), the camera creates a new-data object to be transferred to the image server via cell phone that includes thumbnails, metadata associated with the image and the image data captured by the camera. In some instances, Kahn refers to "a client-side embedded applet" as an "upload program". Kahn, [0062], FIG. 4. A POSITA would have understood that the upload program and the applet are interchangeably used because the upload program (similar to applet) "would be embedded as an application in a device run-time environment, such as J2ME (Sun Microsystems) or BREW (QUALCOMM)." Kahn, [0062].

751. Kahn teaches, "the upload program 410 [also] communicates with the camera memory/API 430, so that **the upload program 410 can retrieve images from the camera**." Kahn, [0063]. A POSITA would have understood that while images from the camera, the upload program also retrieves the associated image data (for example, metadata, thumbnail). Subsequently, at the cell phone, the "upload program 410 **assembles the image data for the images and the corresponding metadata** comprising location information and user (identity) information." Kahn, [0064]. Further, the upload program "establishes an Internet **connection to the server, for example, using HTTP protocol**," Kahn, [0056]. The applet is then responsible for "transmit[ting] all of that [assembled]

information/data to the image management server, via its communication with the server-side application 440." Kahn, [0064].

752. A POSITA would have understood that assembling the image data would constitute processing of image data images from the camera would involve processing the received new-data object in accordance with the HTTP so that the data object can be transmitted over the internet. Id.

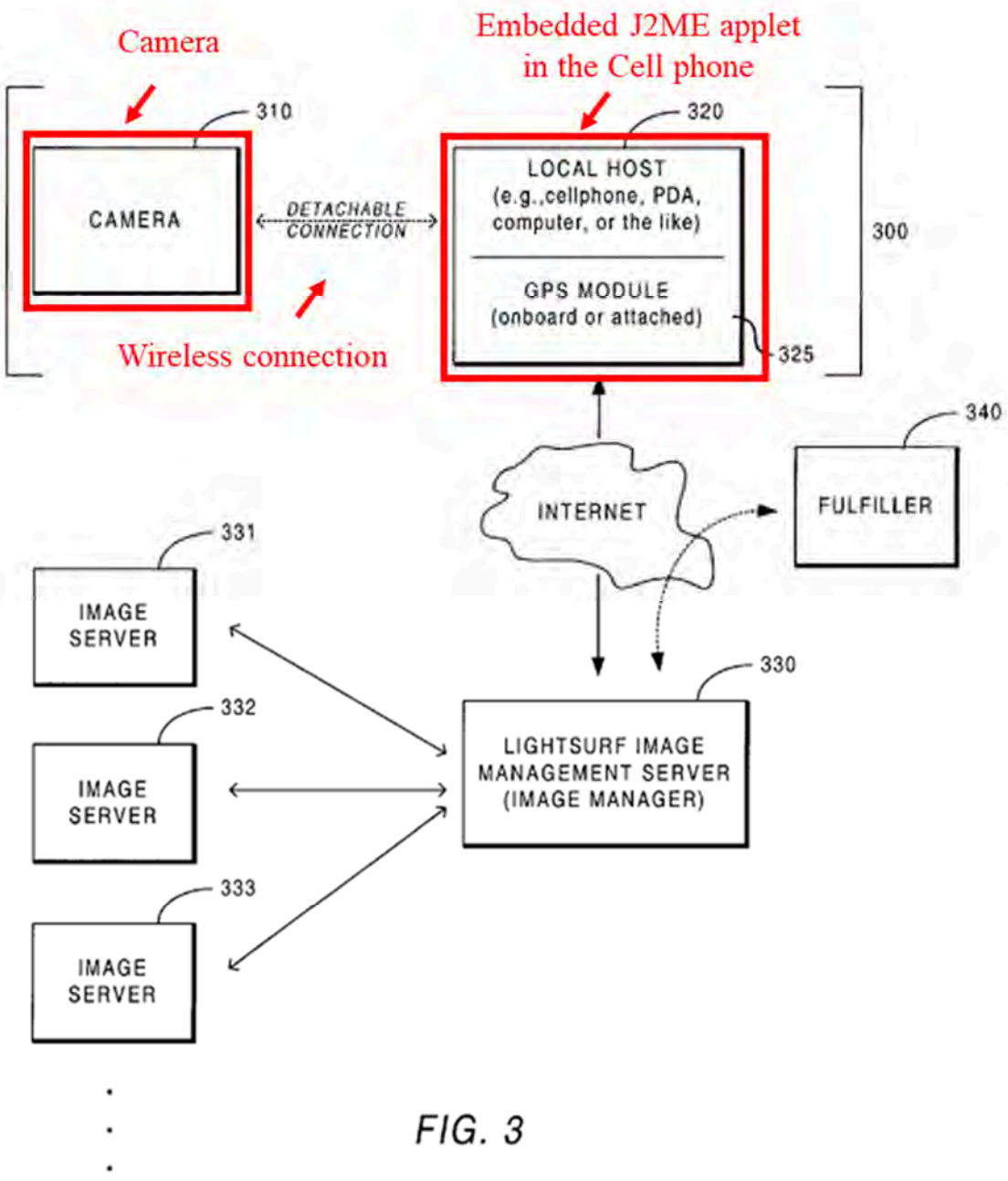


FIG. 3

Kahn, FIG. 3 (annotated).

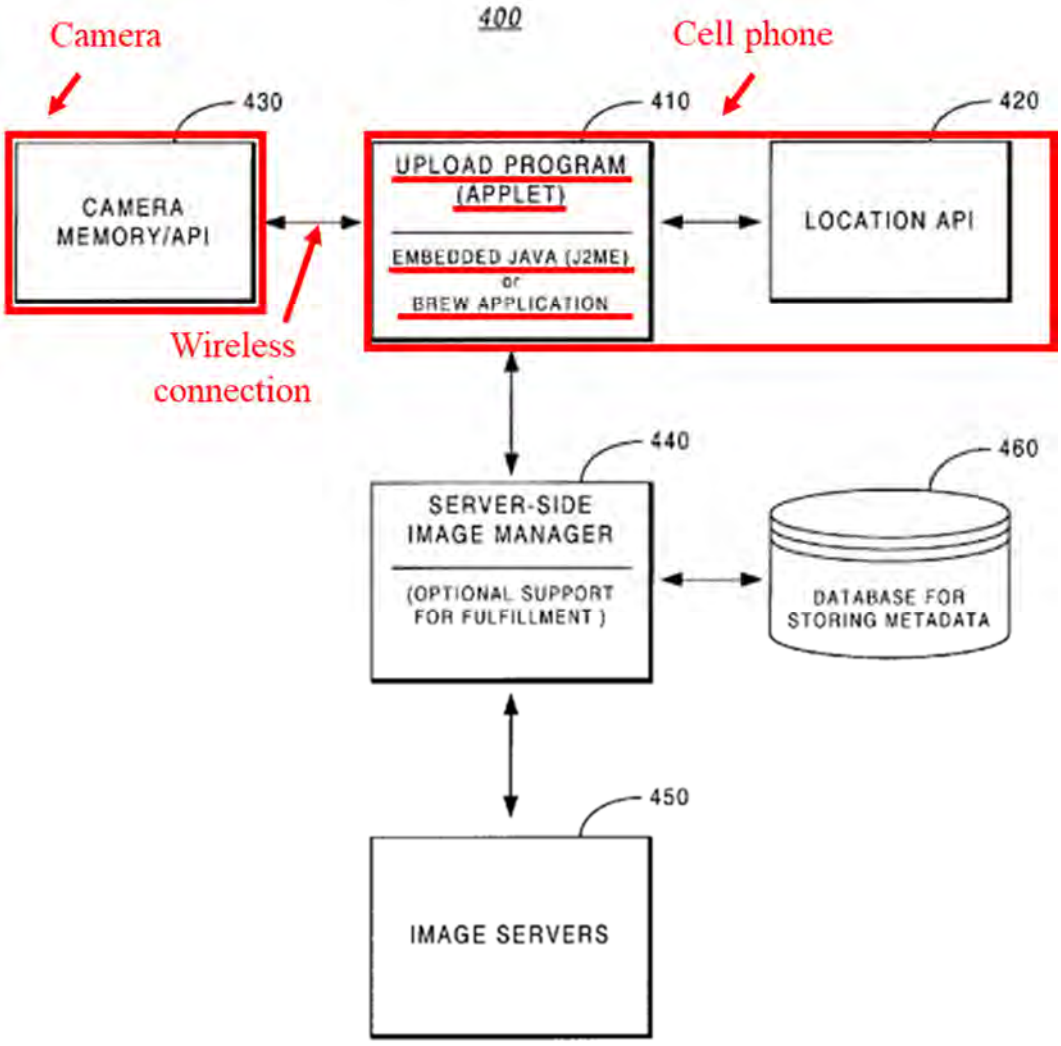


FIG. 4

Kahn, FIG. 4 (annotated).

[1.16.2] and store the received new-data in a memory device of the cryptographically authenticated short-range wireless enabled cellular phone,

753. During uploading process, Kahn teaches "transfer[ing] of the images from the camera to the host (e.g., cell phone), for uploading to a destination image

server." Kahn, [0063]. Kahn also teaches that once the photo is uploaded, the applet deletes the photo from the cell phone's memory. Kahn, [0085] ("step 540, where the photo is deleted (from local storage)."), FIG. 5D (figure element 540). Thus, a POSITA would have understood that in order to delete the photo from the cell phone's memory the photo would have been stored in the first place.

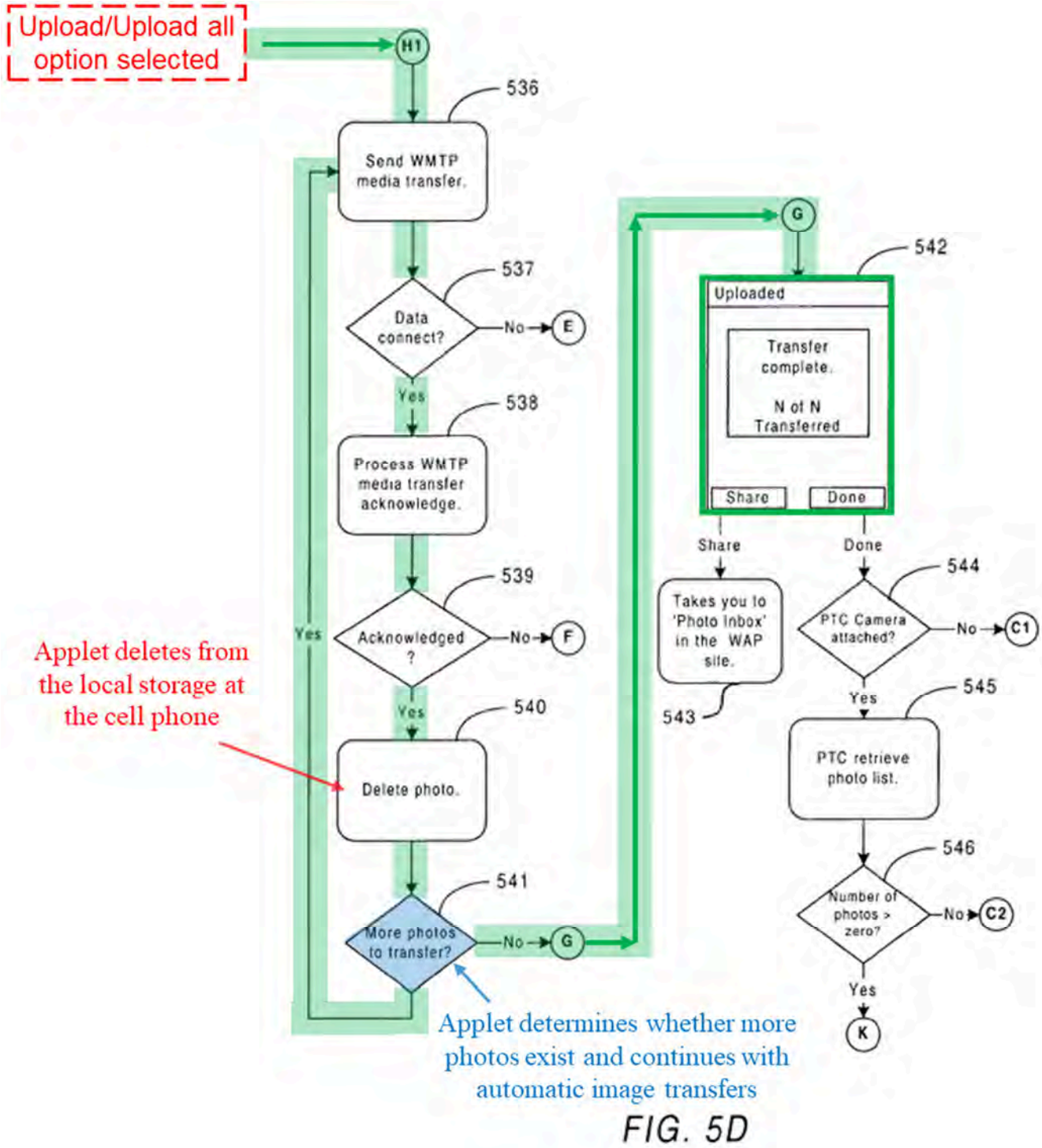


FIG. 5D

Kahn, FIG. 5D (annotated).

[1.17]-[1.18] 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.

754. The Kahn-Feinberg-Bluetooth combination renders obvious [1.17]-[1.18]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests 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.

This limitation is broken down into constituent steps below:

[1.17] 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

755. For example, Kahn discloses "the host device 320 communicates with an online Web-based image management server 330. … the image management server 330 is a Web-based server accessible via the Internet … [i]n order to communicate with the image management server 330, the host device 320 establishes an Internet connection to the server, for example, using HTTP

protocol." Kahn, [0056]. The image management server "allows the system to place images into an online or digital photo album … [s]uch albums may then be accessed by the user (and shared with other users) using Web browser software (e.g., Microsoft Internet Explorer)." Kahn, [0065].

> [0063] In response to a query from **the upload program 410 (e.g., submitted as an HTTP request), the location API 420 returns GPS information indicating the then-current location (e.g., returned as an HTTP response)**. The GPS information may be converted into decimal values (if not in decimal form already) for indicating longitude and latitude. The upload program 410 also communicates with the camera memory/API 430, so that the upload program 410 can retrieve images from the camera. In this manner, **the upload program 410 is able to invoke transfer of the images from the camera to the host (e.g., cell phone), for uploading to a destination image server.**
>
> [0064] The upload program 410 communicates with the server-side image manager 440, which represents server-side program logic typically implemented at a server (e.g., image management server 330) responsible for image organization (including naming and metadata management). The underlying images themselves will be stored via image servers module 450 (which corresponds to image servers 331, 332, 333) that are in communication with the server-side application 440. The upload program 410 assembles the image data for the images and the corresponding metadata comprising location information and user (identity) information, and then transmits all of that information/data to the image management server, via its communication with the server-side application 440. The file path to an individual image and the metadata/attributes of that image are stored in a

corresponding data record in the database 460, which may be implemented using an Oracle database server or the like. Oracle database software is available from Oracle Corporation of Redwood Shores, Calif. **At the completion of upload, image data has been stored at an image server and corresponding metadata information (which now contains the location ID information) has been stored at the database 460.**

Kahn, [0063]-[0064].

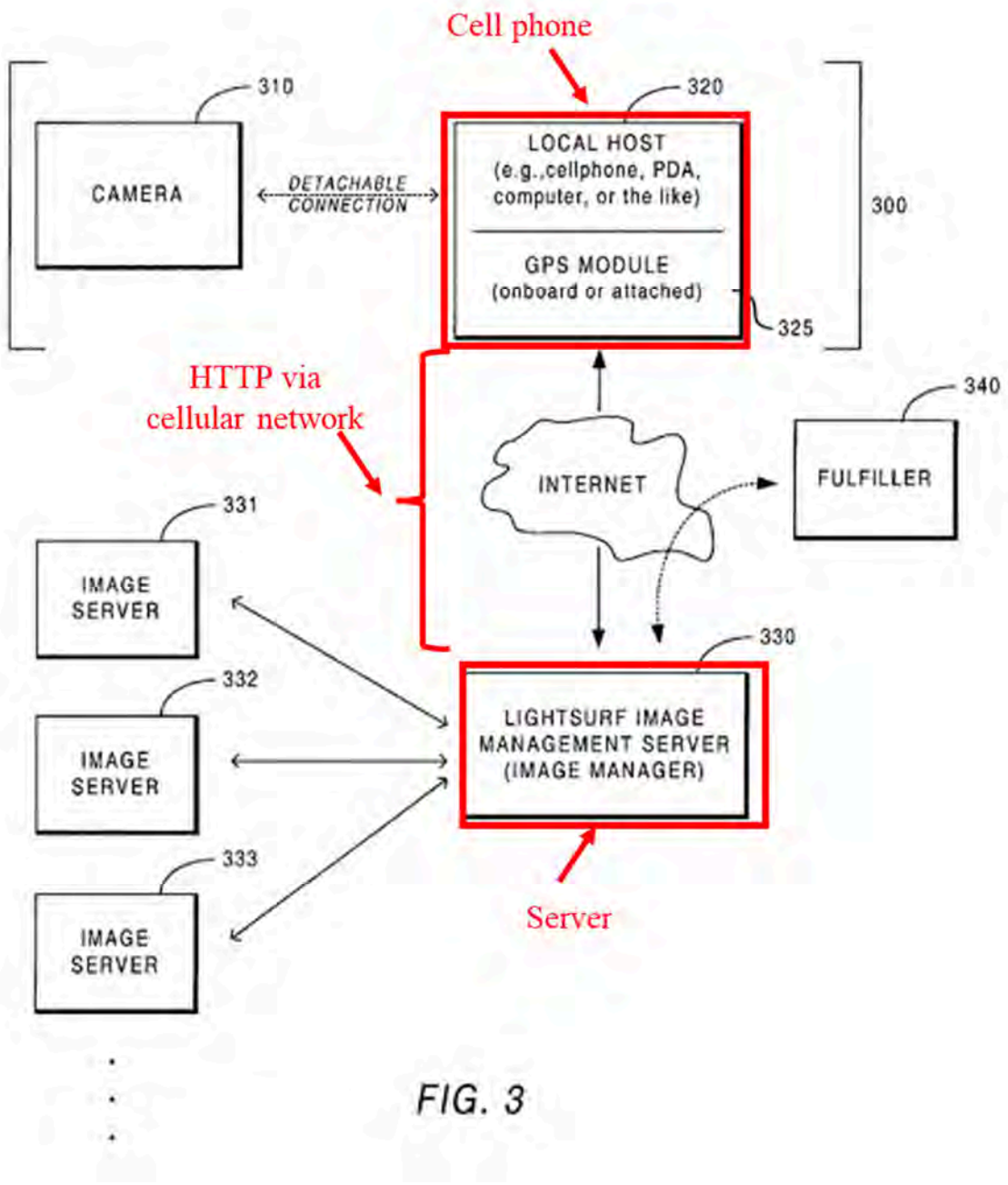


FIG. 3

FIG. 3 (annotated). Kahn, [0023] ("FIG. 3 is a high-level block diagram illustrating the basic components that comprise the environment in which the present embodiment may be implemented.")

[1.18] 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.

756. Kahn teaches "[t]he upload program 410 assembles the image data for the images and the corresponding **metadata comprising** location information and **user (identity) information**" and then "transmits all of that information/data to the image management server." Kahn, [0063]-[0064]. Kahn also teaches "[t]he 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)." Kahn, [0098] (emphasis added.) A POSITA would have understood that this user information included in the metadata is integral to the operation of the user data publishing website, as it uniquely identifies a particular user. Kahn, [0063], [0098].

757. Kahn also teaches that system is configured "place images into an online or digital photo album." Kahn, [0065]. Additionally, Kahn specifies that a "user is **given access to photos** on the camera or **on photo albums (e.g., online photos)**." Kahn, [0074]. However, this access is contingent upon the validity of the user credentials. Kahn, [0082], [0084], FIG. 5C (elements 522, 526) . For example, Kahn discloses that "the applet [at the cell phone] retrieves the NAI and password" from the cell phone's memory and transmits the login credentials "to the photo site (Web-based server providing image management)" to determine the

validity of the user credentials. Kahn, [0082]. Post-upload, Kahn teaches that the user is provided with an option to either "share" or keep the album private. Kahn, [0086] (""the user can select to "Share" the photos, **or simply select "Done"**"), FIG. 5D (figure element 542). Moreover, Kahn teaches that publication of "[s]uch albums may then be **accessed by the user** (**and shared with other users**) using Web browser software (e.g., Microsoft Internet Explorer)." Kahn, [0065]. In light of Kahn's teachings, it would be evident to a POSITA that without sharing the albums not shared would be exclusively available for private consumption on the user's account on the website. Kahn, [0086], FIG. 5D (figure element 542).

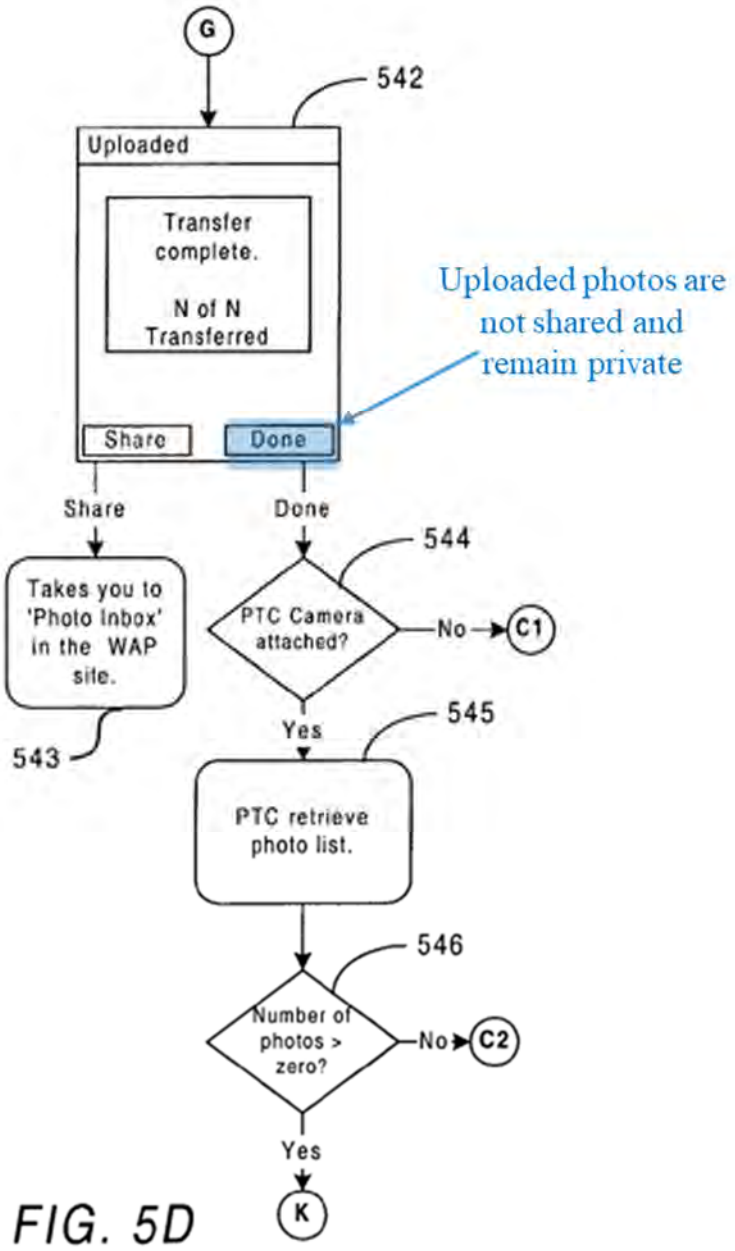


FIG. 5D

Kahn, FIG. 5D (annotated).

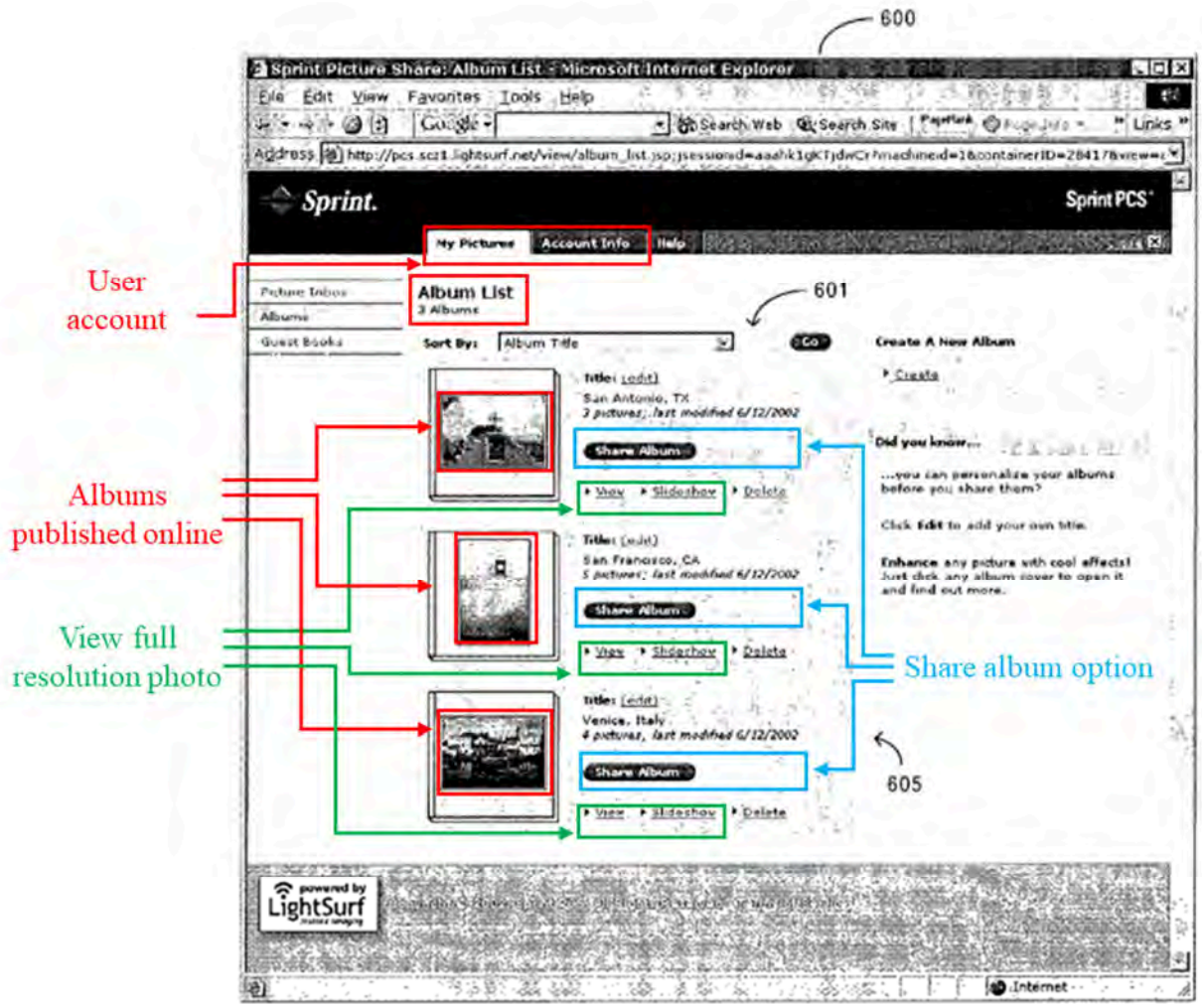


FIG. 6

Kahn, Fig. 6 (annotated).

Claim 13

[13.P] A system, comprising:

758. To the extent the preamble is limiting, The Kahn-Feinberg-Bluetooth combination renders obvious [13.P]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a system. Supra [1.P]. For example, Kahn teaches a "system

300 includes a camera device 310, a host device 320, and a GPS (Global Positioning System) module 325." Kahn, [0055]. Further, "the host device 320 communicates with an online Web-based image management server 330… accessible via the Internet." Kahn, [0056].

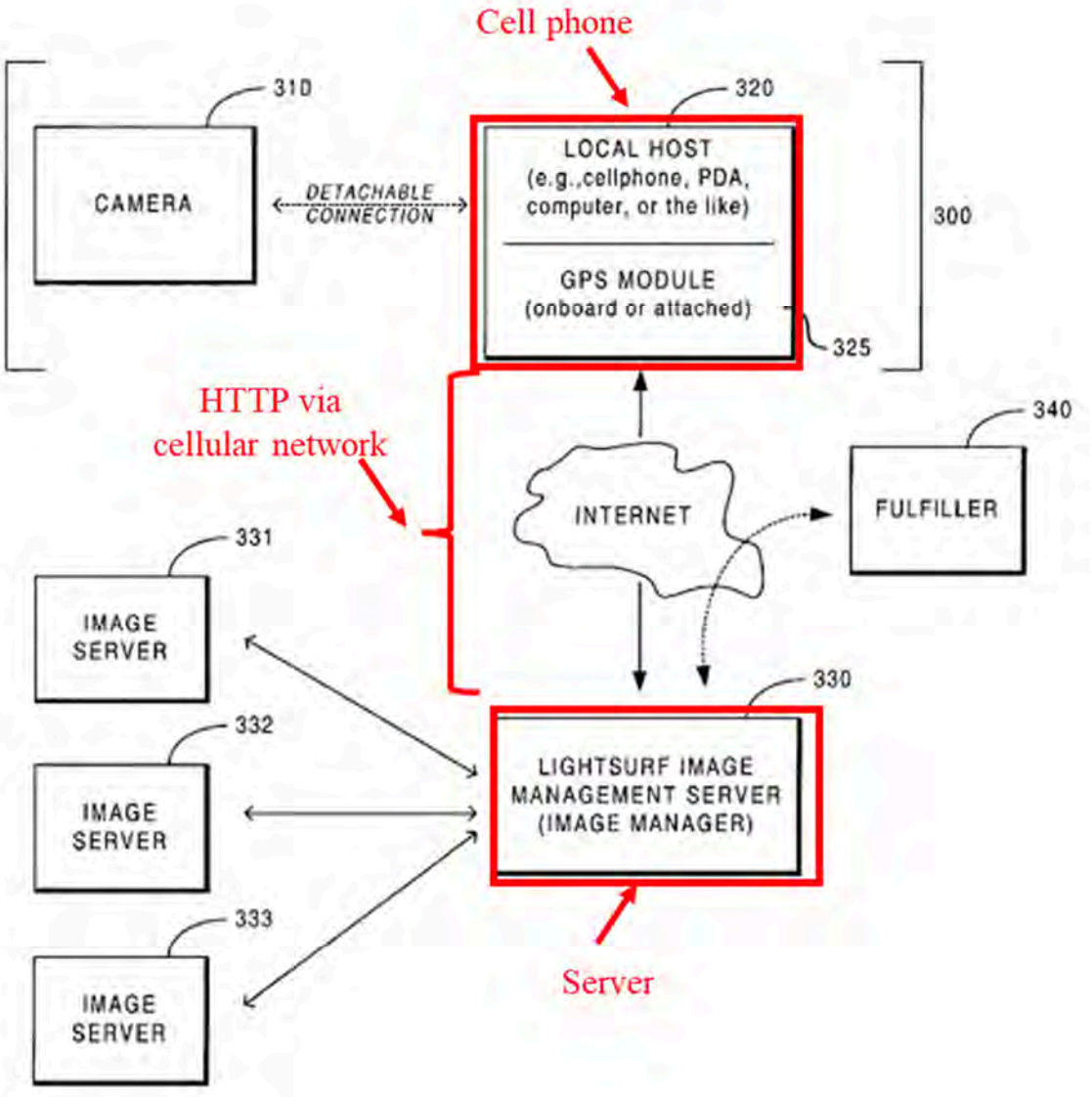


FIG. 3

Kahn, FIG. 3 (annotated).

759. In FIG. 4, Kahn "illustrates implementation of underlying functionality (i.e., processes) in the various modules of FIG. 3." Kahn, [0062]. The "system 400 includes the following functional modules: upload program 410, location API 420, camera memory/API 430, server-side image manager application 440, image servers 450, and database (e.g., Oracle) 460 for storing metadata information." Kahn, [0062].

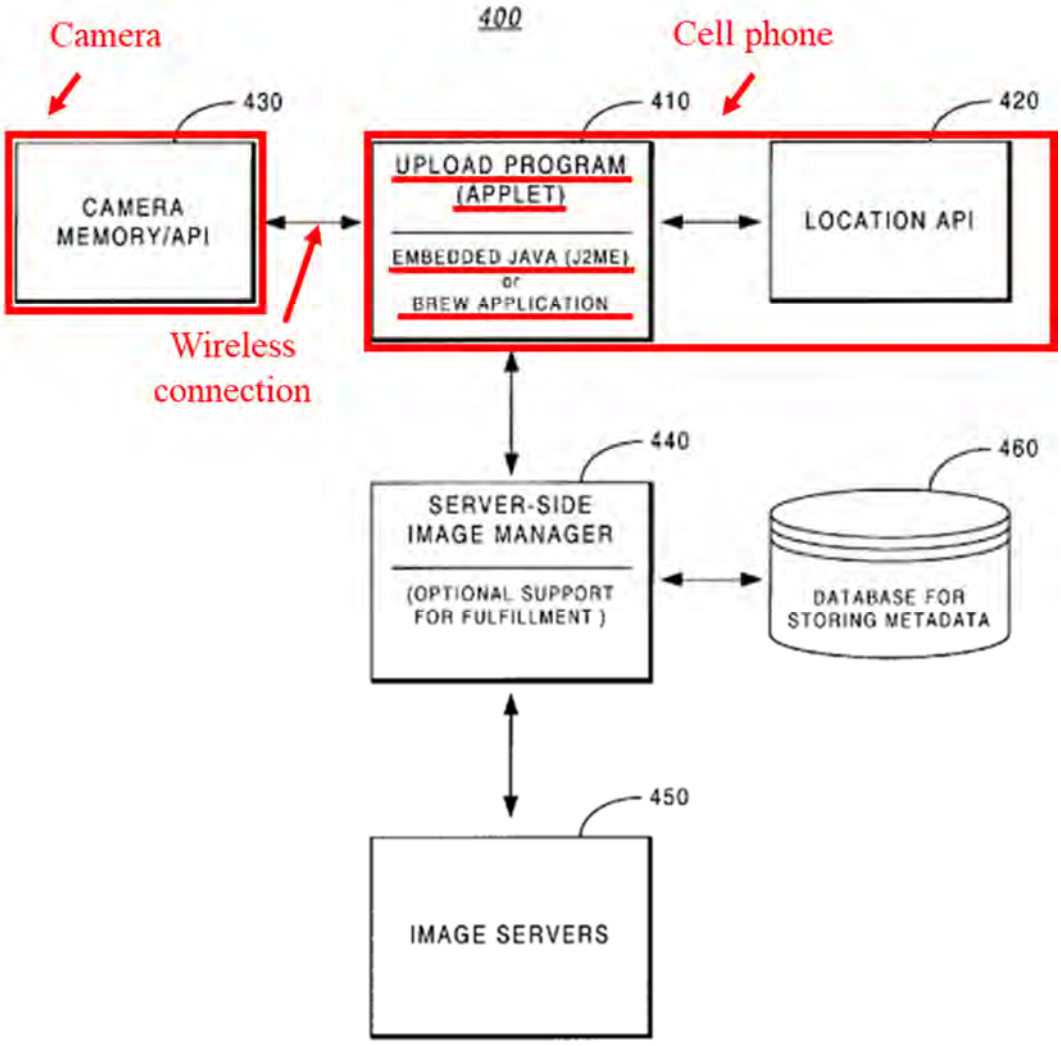


FIG. 4

Kahn, FIG. 4 (annotated).

[13.1] a short-range wireless enabled data capture device, comprising:

760. The Kahn-Feinberg-Bluetooth combination renders obvious [13.1]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a short-range wireless enabled data capture device. Supra [1.P].

[13.2] a first memory device;

761. The Kahn-Feinberg-Bluetooth combination renders obvious [13.2]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a first memory device. Supra [1.1].

[13.3] a first processor coupled to the first memory device;

762. The Kahn-Feinberg-Bluetooth combination renders obvious [13.3]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a first processor coupled to the first memory device. Supra [1.2].

[13.4]-[13.6] a first short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone,
wherein establishing the short-range paired wireless connection comprises cryptographically authenticating identity of the short-range wireless enabled cellular phone, and
wherein establishing the short-range paired wireless connection further comprises the short-range wireless enabled data capture device using an association protocol;

763. The Kahn-Feinberg-Bluetooth combination renders obvious [13.4]-[13.6]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a first short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone, wherein establishing the short-range paired wireless connection comprises cryptographically authenticating identity of the short-range wireless enabled cellular phone, and wherein

establishing the short-range paired wireless connection further comprises the short-range wireless enabled data capture device using an association protocol. Supra [1.3].

[13.7] a data capture circuitry;

764. The Kahn-Feinberg-Bluetooth combination renders obvious [13.7]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a data capture circuitry. Supra [1.6].

[13.8] said first processor configured to acquire new-data using the data capture circuitry,
wherein the new-data is data acquired after the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone is established;

765. The Kahn-Feinberg-Bluetooth combination renders obvious [13.8]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said first processor configured to acquire new-data using the data capture circuitry, wherein the new-data is data acquired after the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone is established. Supra [1.7]-[1.8].

[13.9] said first processor further configured to store the acquired new-data in the first memory device;

766. The Kahn-Feinberg-Bluetooth combination renders obvious [13.9]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said first processor further configured to store the acquired new-data in the first memory device.

Supra [1.9].

[13.10] said processor further configured to create a new-data object, wherein the new-data object comprises:

767. The Kahn-Feinberg-Bluetooth combination renders obvious [13.10]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said processor further configured to create a new-data object. Supra [1.10].

[13.11] signal to notify, wherein the signal to notify corresponds to the acquiring of the new-data for transfer;

768. The Kahn-Feinberg-Bluetooth combination renders obvious [13.11]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests signal to notify, wherein the signal to notify corresponds to the acquiring of the new-data for transfer. Supra [1.11].

[13.12] the acquired new-data; and

769. The Kahn-Feinberg-Bluetooth combination renders obvious [13.1]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests the acquired new-data. Supra [1.12].

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

770. The Kahn-Feinberg-Bluetooth combination renders obvious [13.13]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests associated new-data, wherein the associated new-data corresponds to data associated with the new-data. Supra [1.13].

[13.14]-[13.15] said first processor further configured to receive a data transfer request from the short-range wireless enabled cellular phone, over the established short-range paired wireless connection, wherein the data transfer request is for the acquired new-data that was acquired by the short-range wireless enabled data capture device before receiving the data transfer request; and

771. The Kahn-Feinberg-Bluetooth combination renders obvious [13.14]-[13.15]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said first processor further configured to receive a data transfer request from the short-range wireless enabled cellular phone, over the established short-range paired wireless connection, wherein the data transfer request is for the acquired new-data that was acquired by the short-range wireless enabled data capture device before receiving the data transfer request; and. Supra [1.14].

772. As explained in supra [1.6]-[1.9] the camera acquires and stores new data. Then, the user on the mobile phone can view thumbnails corresponding to the full resolution images as shown in graphical user interface (GUI) mobile screen 550 of FIG. 5E and can select to upload photo(s) in screen 551 and then the camera receives a data transfer request. Kahn discloses that "the upload program 410 is able to invoke transfer of the images from the camera to the host (e.g., cell phone), for uploading to a destination image server." Kahn, [0063]. Kahn teaches that the camera receives a "data transfer request" to transfer new data from the phone's upload program, Kahn, [0063], ("[t]he upload program 410 also communicates with the camera memory/API 430, so that the upload program 410 can retrieve

images from the camera. In this manner, the upload program 410 is able to invoke transfer of the images from the camera to the host (e.g., cell phone), for uploading to a destination image server.”). The graphical user interface (GUI) running on the phone allows the user to select the image(s) to upload as shown in screen 550 and 551 of FIG. 5E. See also supra [1.15].

[13.16] said first processor configured to transfer the new-data object to the short-range wireless enabled cellular phone over the established short-range paired wireless connection;

773. The Kahn-Feinberg-Bluetooth combination renders obvious [13.16]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said first processor configured to transfer the new-data object to the short-range wireless enabled cellular phone over the established short-range paired wireless connection. Supra [1.14].

[13.17] a mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that, when executed by a second processor of the short-range wireless enabled cellular phone controls the second processor to:

774. The Kahn-Feinberg-Bluetooth combination renders obvious [13.17]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a mobile client application for the short-range wireless enabled cellular phone comprising executable instructions executed by a second processor of the short-range wireless enabled cellular phone that controls the second processor.

775. Kahn teaches that “host device 320 may comprise a cellular phone”

and that the cell phone runs a "client-side applet program, which may be embodied as an embedded J2ME applet in the local host.", Kahn, [0055], [0071]. In fact, the user interface of the client side application is shown by Kahn in FIGs. 5A-5F, "a client-side embedded applet (i.e., a small footprint application) that executes method steps and displays exemplary user interface (UI) dialogs/menus for supporting fulfillment.", Kahn, [0071]. A POSITA would understand that in order to execute the client side application, the cell phone would have at least one processor (CPU), memory(s), and other components to execute the client-side applet. As further evidence, Hiroishi teaches that the components of a cell phone include a CPU and memory(s). TTI-1011, [0051], FIG. 3.

[13.18]-[13.19] receive a request through a graphical user interface (GUI) of the cryptographically authenticated short-range wireless enabled cellular phone for new-data and send a data transfer request to the short-range wireless enabled data capture device, over the established short-range paired wireless connection,
wherein the data transfer request is for the acquired new-data that was acquired by the short-range wireless enabled data capture device before receiving the data transfer request;

776. The Kahn-Feinberg-Bluetooth combination renders obvious [13.18]-[13.19]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests receive a request through a graphical user interface (GUI) of the cryptographically authenticated short-range wireless enabled cellular phone for new-data and send a data transfer request to the short-range wireless enabled data capture device, over the established short-range paired wireless connection, wherein the data transfer

request is for the acquired new-data that was acquired by the short-range wireless enabled data capture device before receiving the data transfer request. Supra [13.14]-[13.15], [1.15].

[13.20] receive the new-data object from the short-range wireless enabled data capture device, over the established short-range paired wireless connection;

777. The Kahn-Feinberg-Bluetooth combination renders obvious [13.20]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests receive the new-data object from the short-range wireless enabled data capture device, over the established short-range paired wireless connection. For example, Kahn teaches that "When photos are 'uploaded', they are moved from the camera to the server." via the cellular phone, Kahn, FIGs. 5B, 5E, [0063]. See also Supra [1.10], [1.14].

[13.21] store the new-data received over the established short-range paired wireless connection, in a second memory device of the short-range wireless enabled cellular phone; and

778. The Kahn-Feinberg-Bluetooth combination renders obvious [13.21]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests store the new-data received over the established short-range paired wireless connection, in a second memory device of the short-range wireless enabled cellular phone. As previously stated, For example, Kahn teaches that "When photos are 'uploaded', they are moved from the camera to the server." via the cellular phone, Kahn, FIGs. 5B, 5E, [0063]. Because the images are received from the camera by the cell phone and processed for transmission to the server, the images are stored on the cell phone.

See also Supra [1.16].

[13.22]-[13.23] use HTTP to upload 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.

779. The Kahn-Feinberg-Bluetooth combination renders obvious [13.22]-[13.23]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests use HTTP to upload 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. Supra [1.17]-[1.18].

Claim 9

[9.P] A short-range wireless enabled cellular phone, comprising:

780. To the extent the preamble is limiting, The Kahn-Feinberg-Bluetooth combination renders obvious [9.P]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a short-range wireless enabled cellular phone. For example, Kahn discloses the system 300 as shown in FIG. 3 below that "includes a camera device 310, a host device 320, and a GPS (Global Positioning System) module 325." and that the "host device 320 may comprise a cellular phone, a PDA (personal data assistant) with wireless connectivity, or the like.", Kahn, [0056].

Further Kahn further teaches that “a host device 320 that can be a mobile phone, Kahn, [0045] (“the digital camera 100 would occasionally be connected to a local host device, such as a cellular phone”).

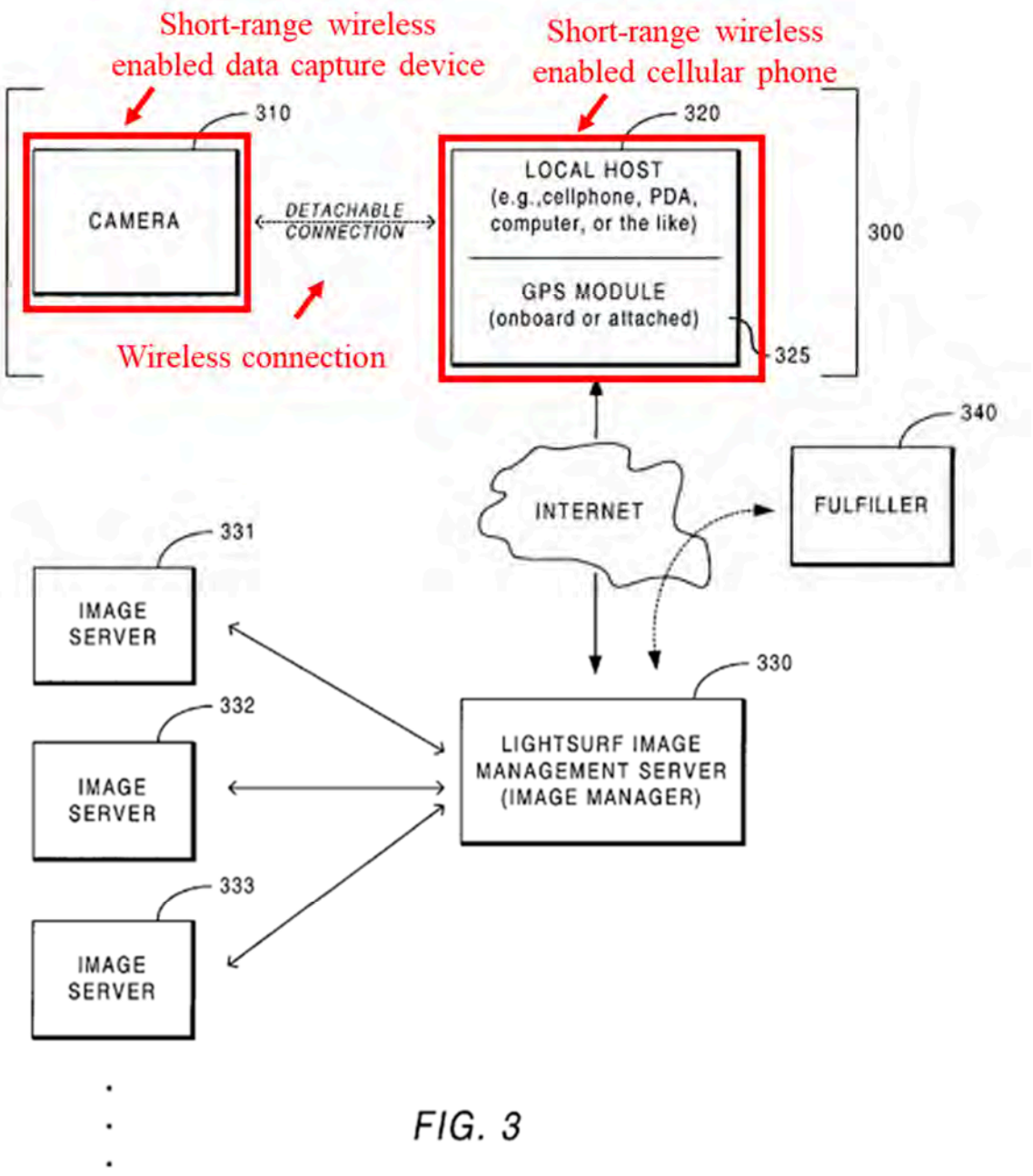


FIG. 3

[9.1] a memory device;

781. The Kahn-Feinberg-Bluetooth combination renders obvious [9.1]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a memory device. Supra [1.16.2].

[9.2] a processor coupled to said memory device;

782. The Kahn-Feinberg-Bluetooth combination renders obvious [9.2]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a processor coupled to said memory device. Supra [13.17].

[9.3] a cellular network communication device configured to connect to internet via a cellular data network;

783. The Kahn-Feinberg-Bluetooth combination renders obvious [9.3]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a cellular network communication device configured to connect to internet via a cellular data network. For example, Kahn discloses "the host device 320 communicates with an online Web-based image management server 330. … the image management server 330 is a Web-based server accessible via the Internet … [i]n order to communicate with the image management server 330, the host device 320 establishes an Internet connection to the server, for example, using HTTP protocol." Kahn, [0056]. See also Supra [9.P].

[9.4]-[9.6] a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range

wireless enabled cellular phone and a short-range wireless enabled data capture device,
wherein the short-range wireless enabled data capture device is configured to cryptographically authenticate identity of the short-range wireless enabled cellular phone when establishing the short-range paired wireless connection, and
wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled mobile device using an association protocol;

784. The Kahn-Feinberg-Bluetooth combination renders obvious [9.4]-[9.6]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled cellular phone and a short-range wireless enabled data capture device, wherein the short-range wireless enabled data capture device is configured to cryptographically authenticate identity of the short-range wireless enabled cellular phone when establishing the short-range paired wireless connection, and wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled mobile device using an association protocol. Supra [1.3].

[9.7] a mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that, when executed by the processor controls the processor to:

785. The Kahn-Feinberg-Bluetooth combination renders obvious [9.7]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a mobile client application for the short-range wireless enabled cellular phone comprising executable instructions executed by the processor. Supra [13.17].

[9.8] receive a new-data object from the short-range wireless enabled data capture device over the established short-range paired wireless connection, wherein the new-data object comprises:

786. The Kahn-Feinberg-Bluetooth combination renders obvious [9.8]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests receiving a new-data object from the short-range wireless enabled data capture device over the established short-range paired wireless connection. Supra [1.10], [13.20].

[9.10]-[9.12] signal to notify and acquired new-data, wherein the acquired new-data is data acquired by the short-range wireless enabled data capture device after the short-range paired wireless connection is established between the short-range wireless enabled cellular phone and the short-range wireless enabled data capture device, and wherein the signal to notify corresponds to the acquiring of the new-data for transfer; and

787. "The Kahn-Feinberg-Bluetooth combination renders obvious [9.10]-[9.12]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests signal to notify and acquired new-data, wherein the acquired new-data is data acquired by the short-range wireless enabled data capture device after the short-range paired wireless connection is established between the short-range wireless enabled cellular phone and the short-range wireless enabled data capture device, and wherein the signal to notify corresponds to the acquiring of the new-data for transfer. Supra [1.7]-[1.12].

[9.13] associated new-data, wherein the associated new-data corresponds to data associated with the new-data;

788. The Kahn-Feinberg-Bluetooth combination renders obvious [9.13]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests associated new-data, wherein the associated new-data corresponds to data associated with the new-data. Supra [1.13].

[9.14] listen and process the signal to notify;

789. The Kahn-Feinberg-Bluetooth combination renders obvious [9.14]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests listen and process the signal to notify. Supra [1.15], [1.16.1].

[9.15] store the received new-data in the memory device; and

790. The Kahn-Feinberg-Bluetooth combination renders obvious [9.1]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests store the received new-data in the memory device. Supra [1.16.2].

[9.16]-[9.17] 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.

791. The Kahn-Feinberg-Bluetooth combination renders obvious [9.16]-[9.17]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests 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. Supra [1.17]-[1.18].

Claim 4

[4.P] A system, comprising:

792. To the extent the preamble is limiting, The Kahn-Feinberg-Bluetooth combination renders obvious [4.P]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a system. Supra [13.P].

[4.1] a data capture device, comprising:

793. The Kahn-Feinberg-Bluetooth combination renders obvious [4.1]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a data capture device. Supra [13.1].

[4.2] a first memory device;

794. The Kahn-Feinberg-Bluetooth combination renders obvious [4.2]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a first memory device. Supra [13.2].

[4.3] a first processor coupled to the first memory device;

795. The Kahn-Feinberg-Bluetooth combination renders obvious [4.3]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a first processor coupled

to the first memory device. Supra [13.3].

[4.4]-[4.6] a first short-range wireless communication device configured to establish a short-range paired wireless connection with an internet connected cellular phone,
wherein establishing the short-range paired wireless connection comprises, the data capture device cryptographically authenticating identity of the cellular phone, and wherein establishing the short-range paired wireless connection further comprises the data capture device using an association protocol;

796. The Kahn-Feinberg-Bluetooth combination renders obvious [4.4]-[4.6]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a first short-range wireless communication device configured to establish a short-range paired wireless connection with an internet connected cellular phone, wherein establishing the short-range paired wireless connection comprises, the data capture device cryptographically authenticating identity of the cellular phone, and wherein establishing the short-range paired wireless connection further comprises the data capture device using an association protocol. Supra [1.3]-[1.5], [13.4]-[13.6].

[4.7] a data capture circuitry;

797. The Kahn-Feinberg-Bluetooth combination renders obvious [4.7]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a data capture circuitry. Supra [1.6], [13.7].

[4.8]-[4.9] said first processor configured to acquire new-data in the data capture device using the data capture circuitry,

wherein the new-data is data acquired after establishing the short-range paired wireless connection with the cellular phone;

798. The Kahn-Feinberg-Bluetooth combination renders obvious [4.8]-[4.9]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said first processor configured to acquire new-data in the data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection with the cellular phone. Supra [1.7]-[1.8], [13.8].

[4.10] said first processor further configured to store the new-data in the first memory device;

799. The Kahn-Feinberg-Bluetooth combination renders obvious [4.10]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said first processor further configured to store the new-data in the first memory device. Supra [1.9], [13.9].

[4.11] said first processor further configured to create a new-data object, wherein the new-data object comprises:

800. The Kahn-Feinberg-Bluetooth combination renders obvious [4.11]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said first processor further configured to create a new-data object. Supra [1.10], [13.10].

[4.12] signal to notify, wherein the signal to notify corresponds to the acquiring of the new-data for transfer to the cryptographically authenticated cellular phone;

801. The Kahn-Feinberg-Bluetooth combination renders obvious [4.12]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests signal to notify, wherein

the signal to notify corresponds to the acquiring of the new-data for transfer to the cryptographically authenticated cellular phone. Supra [1.11], [13.11].

[4.13] the acquired new-data; and

802. The Kahn-Feinberg-Bluetooth combination renders obvious [4.1]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests the acquired new-data; and. Supra [1.12], [13.12].

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

803. The Kahn-Feinberg-Bluetooth combination renders obvious [4.14]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests associated new-data, wherein the associated new-data corresponds to data associated with the new-data. Supra [1.13], [13.13].

[4.15] said first processor further configured to transfer automatically the new-data object to the cryptographically authenticated cellular phone, over the established short-range paired wireless connection;

804. The Kahn-Feinberg-Bluetooth combination renders obvious [4.15]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said first processor further configured to transfer automatically the new-data object to the cryptographically authenticated cellular phone, over the established short-range paired wireless connection. Supra [1.14], [13.16].

[4.16] said cellular phone, comprising:

805. The Kahn-Feinberg-Bluetooth combination renders obvious [4.16]. In

my opinion, Kahn-Feinberg-Bluetooth teaches or suggests said cellular phone. Supra [9.P].

[4.17] a second memory device;

806. The Kahn-Feinberg-Bluetooth combination renders obvious [4.17]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a second memory device. Supra [9.1].

[4.18] a second processor coupled to said second memory device;

807. The Kahn-Feinberg-Bluetooth combination renders obvious [4.18]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a second processor coupled to said second memory device. Supra [9.2].

[4.19] a cellular network communication device configured to connect to the internet via the cellular data network;

808. The Kahn-Feinberg-Bluetooth combination renders obvious [4.19]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a cellular network communication device configured to connect to the internet via the cellular data network. Supra [9.3].

[4.20] a second short-range wireless communication device configured to establish the short-range paired wireless connection between the cellular phone and the data capture device;

809. The Kahn-Feinberg-Bluetooth combination renders obvious [4.20]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a second short-range

wireless communication device (Wireless Radio 24) configured to establish the short-range paired wireless connection between the cellular phone and the data capture device. Feinberg, [0041], Figure 1. *See also* Supra [4.4]-[4.6], [9.4]-[9.6].

[4.21] a mobile client application for the cellular phone comprising executable instructions that, when executed by the second processor controls the second processor to:

810. The Kahn-Feinberg-Bluetooth combination renders obvious [4.21]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a mobile client application for the cellular phone comprising executable instructions executed by the second processor. Supra [9.7].

[4.22] listen for the signal to notify;

811. The Kahn-Feinberg-Bluetooth combination renders obvious [4.22]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests listen for the signal to notify. Supra [9.14].

[4.23] receive the new-data object from the data capture device;

812. The Kahn-Feinberg-Bluetooth combination renders obvious [4.2]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests receive the new-data object from the data capture device. Supra [9.8]-[9.9].

[4.24] store the received new-data in the second memory device; and

813. The Kahn-Feinberg-Bluetooth combination renders obvious [4.24]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests store the received new-data in the second memory device. Supra [9.15].

[4.25]-[4.26] 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.

814. The Kahn-Feinberg-Bluetooth combination renders obvious [4.25]-[4.26]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests 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. Supra [9.16]-[9.17].

Claim 2

[2] The short-range wireless enabled data capture device of claim 1, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

815. The Kahn-Feinberg-Bluetooth combination renders obvious [2]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing. Supra [1.3].

Claim 3

[3] The short-range wireless enabled data capture device of claim 1, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.

816. The Kahn-Feinberg-Bluetooth combination renders obvious [3]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data. For example, as discussed above (supra [1.7]-[1.8]), Kahn teaches capturing images (acquiring new-data), for example in step 701 of FIG. 7. During the image capturing process, Kahn also teaches acquiring associated new data that is also digital data such as GPS location information and time stamp information., Kahn, [0058], [0008], [0098].

Claim 5

[5] The system of claim 4, wherein establishing the short-range paired wireless connection comprises the data capture device using an association protocol.

817. The Kahn-Feinberg-Bluetooth combination renders obvious [5]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests establishing the short-range paired wireless connection comprises the data capture device using an association protocol. Supra [1.3].

Claim 6

[6] The system of claim 4, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

818. The Kahn-Feinberg-Bluetooth combination renders obvious [6]. In

my opinion, Kahn-Feinberg-Bluetooth teaches or suggests the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing. Supra [2].

Claim 7

[7] The system of claim 4, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.

819. The Kahn-Feinberg-Bluetooth combination renders obvious [7]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data. Supra [3].

Claim 8

[8] The system of claim 4, wherein a graphical user interface (GUI) is provided in the cryptographically authenticated cellular phone, and wherein the graphical user interface (GUI) is for the received new-data.

820. The Kahn-Feinberg-Bluetooth combination renders obvious [8]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a graphical user interface (GUI) is provided in the cryptographically authenticated cellular phone, and wherein the graphical user interface (GUI) is for the received new-data. For example, Kahn illustrates, in "FIGS. 5A-F illustrate execution of a client-side embedded applet (i.e., a small footprint application) that executes method steps and displays exemplary user interface (UI) dialogs/menus for supporting fulfillment."

Kahn, [0025], [0070]-[0071], FIGs. 5A-F. See Ground 2A, [1.7]-[1.14].

Claim 10

[10] The short-range wireless enabled cellular phone of claim 9, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

821. The Kahn-Feinberg-Bluetooth combination renders obvious [10]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing. Supra [2], [6].

Claim 11

[11] The short-range wireless enabled cellular phone of claim 9, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.

822. The Kahn-Feinberg-Bluetooth combination renders obvious [11]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data. Supra [3].

Claim 12

[12] The short-range wireless enabled cellular phone of claim 9, wherein a graphical user interface (GUI) is provided in the cryptographically authenticated short-range wireless enabled cellular phone, and wherein the graphical user interface (GUI) is for the received new-data.

823. The Kahn-Feinberg-Bluetooth combination renders obvious [12]. In

my opinion, Kahn-Feinberg-Bluetooth teaches or suggests a graphical user interface (GUI) is provided in the cryptographically authenticated short-range wireless enabled cellular phone, and wherein the graphical user interface (GUI) is for the received new-data. Supra [8].

Claim 14

[14] The system of claim 13, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

824. The Kahn-Feinberg-Bluetooth combination renders obvious [14]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing. Supra [2].

Claim 15

[15] The system of claim 13, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.

825. The Kahn-Feinberg-Bluetooth combination renders obvious [15]. In my opinion, Kahn-Feinberg-Bluetooth teaches or suggests 15. The system of claim 13, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data. Supra [6].

XII. INVALIDITY ANALYSIS OF THE '121 PATENT

A. Ground 1: Hiroishi in view of Kahn, Endsley, and Bluetooth renders claims 1-10 obvious

826. In the proposed combination, as described by Hiroishi, a photograph system that includes a cellular phone that connects to a camera via a Bluetooth connection. *See, e.g.*, TTI-1011, [0042], [0066]-[0067]. The cellular phone controls the camera to capture images, store images, and transmit images to the cellular phone. *Id*., [0068]. The cellular phone then transmits images to a remote computer destination by a cellular network connection via the Internet. *Id*., [0105]-[0112]. In the combination, the mobile phone is configured, as taught by Kahn, to use HTTP to send images, a user authentication credential, and a user preference that includes GPS information. Also, in the combination, the timing of the transmission of the images to the print shop (or other remote terminal) as described by Hiroishi is controlled based on a determination of a time period for transmission, in manner similar to what is described by Endsley.

827. If necessary, in the combination, the cellular phone uses a touch-based GUI and/or a timestamp signal sent from the digital camera to the mobile phone corresponding to the acquired new-data as taught by Kahn. In the combination, the mobile phone transfers the images with the timestamp to the remote terminals using a packet compliant with HTTP, which requires that the mobile phone process the timestamp to create the HTTP compliant packet.

1. The Predictable Combination of Hiroishi, Kahn, and Endsley

828. A POSITA at the time of the invention would have been motivated to combine the teachings of Hiroishi, Kahn, and Endsley thus rendering the subject matter of the ’121 patent challenged claims (claims 1-10) obvious.

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

830. Hiroishi and Kahn are also pertinent to the problem of the ’121 patent: transmission of image data by a cellular phone that was captured by a digital camera. TTI-1001, Background. Hiroishi addresses this problem through Bluetooth wireless data transmission and software-based control of the digital camera from the mobile device. *See, e.g.*, Hiroishi, [0043], [0053], [0061]. Kahn addresses the problem through efficient publishing of image data from a cellular phone to a website using HTTP. *See, e.g.*, Kahn, [0056], [0063].

831. Second, a POSITA would have been motivated to use Kahn's upload technique to publish image data received at the mobile device of Hiroishi. At the time of the alleged Critical Date, photo-sharing websites and personal blogs had become ubiquitous. *See, e.g.*, TTI-1020, 3:25-49, 4:47-67; TTI-1021, 5:49-56 (describing use HTTP to send images from the phone to the server). Websites like FLICKR, PHOTOBUCKET, and PICASA allowed users to publish photographs and share them with friends, colleagues, and internet users. *See, e.g.*, TTI-2018, 5:25-28; TTI-1022, [0032].

832. Cellular phones had also become ubiquitous. The original iPhone was released six months before the provisional filing date of the '121 patent (the iPhone was released on June 29, 2007), and years before that companies like Blackberry, Motorola, and Nokia had developed cellular phones that allowed users to transfer image data over the Internet. *See e.g.*, Hiroishi, [0015], [0047], FIG. 2. The '121 patent even refers to mobile phones as "ubiquitous." '121 patent, 10:15-16 ("The mobile device 202 may, for example, be a **ubiquitous mobile phone**.") (emphasis added). Kahn also teaches a camera wirelessly connected to a mobile phone for capturing images and uploading images to a remote server. *See, e.g.*, Kahn, [0045], [0055].

833. Kahn recognizes both of these trends and teaches an efficient and predictable technique for uploading image data (captured by a camera) from a

mobile device to a publishing website. *See, e.g.*, Kahn, [0063].

834. The teachings of Kahn would have provided straightforward benefit to the user of the mobile device in Hiroishi: predictable upload of image files and an action setting using an existing HTTP connection between the mobile device and a remote (publishing) server. Hiroishi already teaches the desire to transfer image data from a digital camera to a mobile device to a terminal device. *See, e.g.*, Hiroishi, [0044]. Kahn would have furthered this purpose by allowing the user to share image data over the Internet in a straight-forward and well-known way.

835. Third, there would have been a reasonable expectation of success in combining the teachings of Hiroishi and Kahn. The combination would have required simply packaging the image data from the mobile device of Hiroishi in an HTTP message as Kahn teaches as was a well-known method at the time for packet data transfer over the Internet. Both modifications would have been well within the ability of a POSITA. It would also have been obvious to modify Hiroishi to send the action setting, such as the number of pages or schedule for pick-up, using HTTP, in a manner similar to that described by Kahn. To the extent that the action setting of Hiroishi is insufficient to meet the limitation, it would have been obvious to modify Hiroishi with an action setting, like that of Kahn. For example, it would have been obvious to modify Hiroishi to send an action setting with the images using HTTP to create a new album for the images to be viewed at

a friend's terminal or the user's terminal. Doing so would have allowed the user to record the images remotely using the well-known and efficient Internet transfer protocol of HTTP used by Kahn.

836. Fourth, to the extent that the user identifier is interpreted to be the identifier of the user of the mobile phone, a POSITA would have found it obvious to include the user identifier with the images when transferring the images to the remote internet server. *See, e.g.*, Kahn, [0098]. This way, a POSITA would recognize the advantage of being able to uniquely identify the owner of the images, e.g., using a database field for user ID. Kahn, [0098]. In the example scenario of Hiroishi's print shop, the print shop worker can quickly and easily identify the owner of the images by the file name, and can validate the owner when providing the printed images. Likewise, the fulfillment center worker of Kahn can easily identify the owner of the images.

837. A POSITA would have been motivated, and found it obvious, to store a user authentication credential at the cellular phone and send the user authentication credential to the publishing web service using HTTP. Hiroishi already teaches that the email address of the destination terminal is used to send images to the destination terminal. *See, e.g.*, Hiroishi, [0110]. Because the '121 patent claims do not require that the user authentication credential uniquely identifies the operator of the mobile phone, Hiroishi alone would invalidate this

feature. For example, claim 3 recites that the user authentication credential "is used to authenticate a user on the user data publishing website and publish the new-data for private use on the user data publishing website." '121 patent, claim 3. Likewise, claim 6 states that the user authentication credential "is for a user of the user data publishing website." *Id*., claim 6. The claims leave ambiguous which user the user authentication credential belongs to. In Hiroishi, the email address of the print shop or other terminal unit satisfies this limitation. *See, e.g.*, Hiroishi, [0110].

838. A POSITA would have also been motivated to combine Hiroishi to include the location ID (GPS information) of the camera sent with the images to the remote server, in a manner similar to that taught by Kahn, which includes global positioning information with the images transferred from the mobile phone to the server. Hiroishi describes sending the images from the phone to a print shop. *See, e.g*., Hiroishi, [0049]. In the combination, a POSITA would have recognized the advantage of providing current location information to identify a print shop (Kahn's fulfillment center) that was close by. *See, e.g.*, Kahn, [0094]; Hiroishi, [0122] ("the mobile phone 40 may be provided with a WWW (World Wide Web) browser, wherein this browser allows a user to search the terminal unit 20 installed at the print shop located at the location nearest to a photographing site and to order a print. This improves convenience since a print can be ordered from

a nearby print shop"). Furthermore, a POSITA would have known the advantage of including location information with the images would add to the later viewing enjoyment of the pictures by the location reminder of each photograph. *See, e.g.*, Kahn, [0012] (describing the advantages of associating location information with images).

839. In addition, a POSITA would have been motivated to include location information from a global positioning system (GPS) module with the photographs to avoid later having to take steps to associate the photos with location information using a time-stamp method. *See, e.g.*, Kahn, [0060]. By associating the images with the GPS location information when they are taken, or shortly thereafter, the photograph system of Hiroishi would include the benefits of location information with the images without adding steps requiring computational resources. Likewise, performing the timestamp process would also introduce inaccuracies to the location association for the images. By performing the location association when the images are taken, as suggested by Kahn, the location for each image would be more accurate. In a similar vein, the image locations would also be more specific. *See e.g.*, Kahn, [0065].

840. A POSITA would have found it obvious to modify Hiroishi to include timestamp information with the image data, as was a well known technique at the time. TTI-1017, [0008] (describing "prior art imaging devices have only been able

to record information about date/time (timestamp) that an image was captured"), [0060] (describing that "the image data already includes timestamp information (i.e., timestamp indicating when the image is captured"). Kahn makes it clear that timestamp information being included with image data was a well-known technique for recording the date and time of when an image was captured. TTI-1017, [0008], [0060].

841. A POSITA would have been motivated to include the timestamp information with the image data of Hiroishi to record the date and time of when the images were captured. The date and time would provide information to the user to later correlated images with when those images were taken, for posterity. *Id*. In addition, as explained by Kahn, the timestamp information could also be used to correlate location information with the images, "by matching timestamps of the various images against the system's time-correlated historical location information." TTI-1017, [0060]. As already discussed, a POSITA would have known that having the location of the images would help in identifying a near-by print shop, in addition to enhancing the user's photographing experience and memories.

842. A POSITA would recognize the benefits of a touch-based GUI, like that of Kahn, for operating the mobile phone to control the camera in Hiroishi. TTI-1017, FIG. 5A-F. For example, a touch-based GUI would allow the selection

of changing buttons faster. In addition, the touch-based GUI would enhance the user experience by allowing the user to interact directly with the images on the screen. *Id*.

843. A POSITA would have found it obvious to modify Hiroishi to control the transfer the images sent by the mobile phone of Hiroshi to the remote terminal based on a timer setting, as described in Endsley. *See, e.g.*, TTI-1024, [0048], [0055]. In the combination, the transmission of the images to the print shop (or other remote terminal) as described by Hiroishi is delayed based on a determination of a time, in manner similar to what is described by Endsley. In Endsley, the communication device can "wait to initiate data transfer until a predetermined time when transmission rates are low or use of the transmission network by the consumer is unlikely." Endsley, [0055]; *see also id*., [0048]. By waiting to transmit the images to the print shop, the transmission of data can be accomplished "on the basis of lowest transmission rates, volume of data being received at the service provider, or unlikely utilization of the transmission network by the consumer" *Id*., [0055] (describing choosing transmission times (periods) that are "unlikely to interference with other consumer usage"). Put simply, a POSITA would have recognized that the transmission of images from the mobile phone to the remote terminal in Hiroishi would have benefited from choosing a transmission time that would result in lower transmission rates and higher

likelihood of success.

844. A POSITA would have had a reasonable expectation of success implementing the transmission scheme in the combination because doing so would have relied on 1) an internal clock of the mobile phone, which was well known feature at the time; and 2) statistics and other telemetry about the network. Endsley describes that the communication device would include an "internal clock" for transmitting data "at certain designated time periods." For example, "data may be transmitted only at off hours . . . when transmission rates are low and there is a relatively lower chance of disruption to the user in the use of the network system." Endsley, [0048] ("It is of course understood that the communication device 20 may be programmed for allowing transmission during at [sic] any desired time period.").

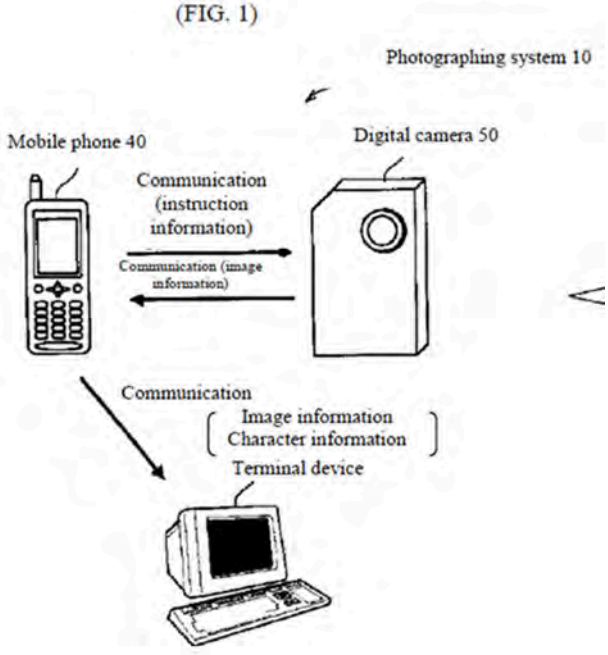
845. Finally, because Hiroishi relies on Bluetooth, a POSITA would have been motivated to look to Bluetooth (the Bluetooth standard 2.1) for more information on the implementation and features of Bluetooth. To the extent that the Bluetooth features are not inherent or envisaged by a skilled artisan reading Hiroishi, it would have been obvious to use the details disclosed in Bluetooth with a system like Hiroishi, which states that Bluetooth is used for local wireless communication. In the combination, a POSITA would use the features disclosed in Bluetooth.

2. Analysis

Claim 7

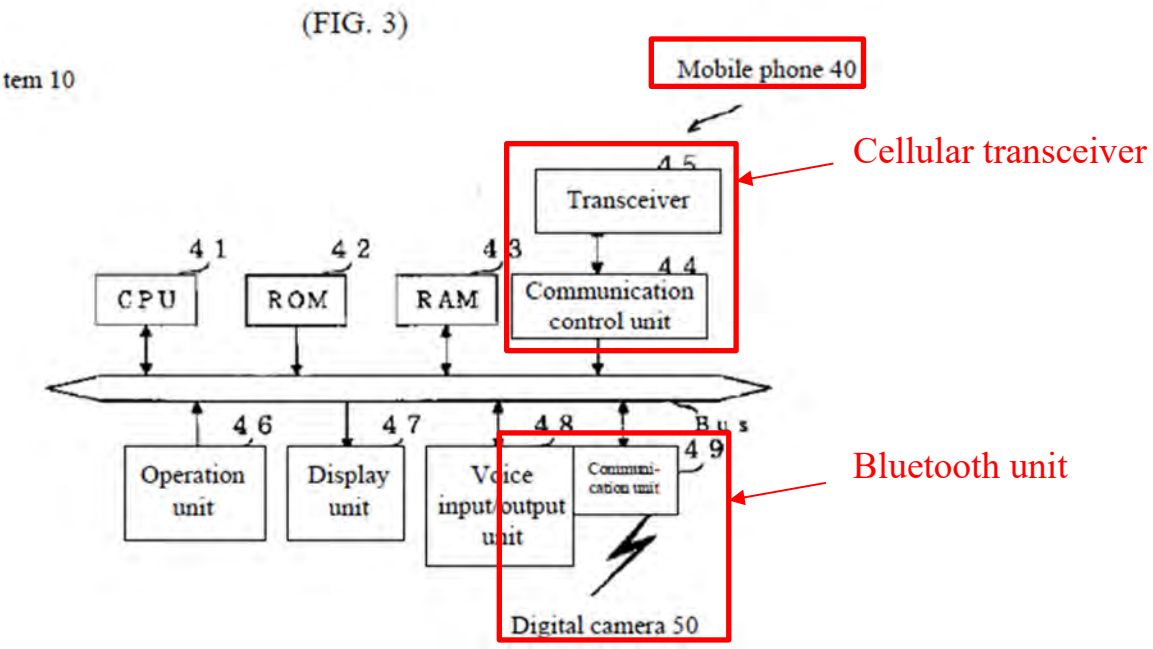
[7.P] A short-range wireless enabled cellular phone, comprising:

846. To the extent the preamble is limiting, the Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [7.P]. The Hiroishi-Kahn-Endsley-Bluetooth combination teaches a short-range wireless enabled cellular phone. Hiroishi, FIG. 1, [0043]-[0044]. Hiroishi discloses a "photographing system 10 according to this embodiment is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth. Bluetooth is a wireless transfer standard that uses a 2.4 GHz bandwidth and does not require any license to use, and can perform transfer of data signals in the range within about 10 m." *Id*., [0066].



Hiroishi, FIG. 1.

847. Hiroishi teaches that the mobile phone 40 includes a "communication control unit 44 is connected to a transceiver 45 for modulating carrier waves by the voice data for transmission or packet information under the control of the communication control unit 44, using these as a radio signal for the transmission from an antenna, and demodulating the radio signal received from the antenna to restore the voice data or packet information." used for making telephone calls. Hiroishi, [0052].



Hiroishi, FIG. 3 (annotated)

848. A POSITA would have recognized that the communication control

unit and transceiver in Hiroishi were for communicating across a cellular network, thereby making the mobile phone 40 a cellular phone. *See, e.g.*, Hiroishi, [0052], FIGS. 2-3; see also *id*., [0048] (describing telephone networks 16A and 16B as including a "Personal Digital Cellular" network).

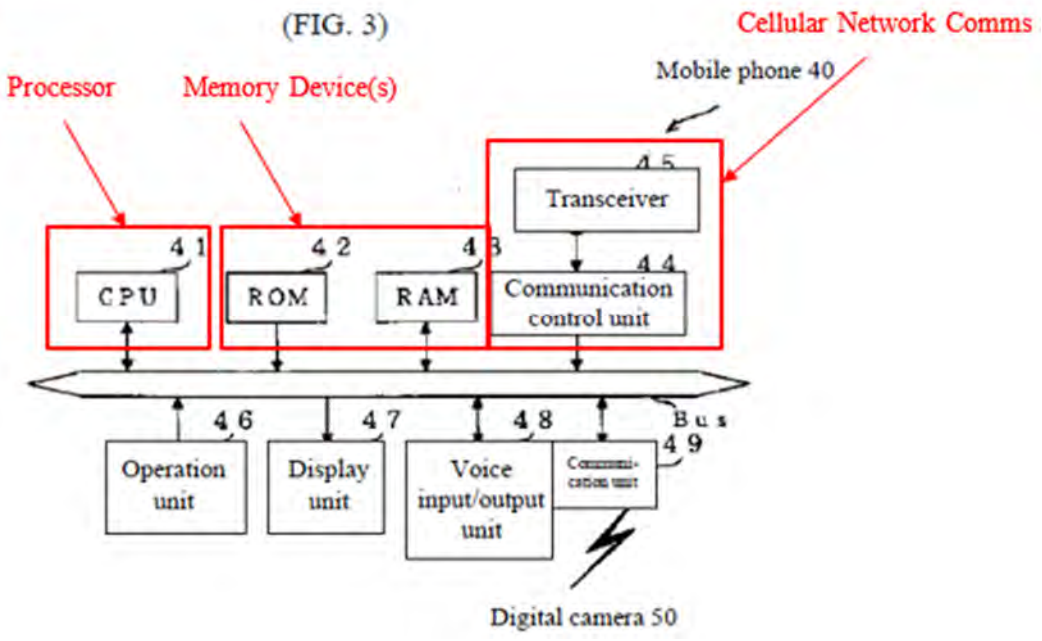
849. In addition, as shown in FIG. 3 above, Hiroshi teaches a "communication unit 49 for carrying out a communication corresponding to a predetermined communication protocol with the digital camera 50." Hiroishi, [0051]. "[T]he communication unit 49 of the mobile phone 40 and the communication unit 59 of the digital camera 50 are configured so as to allow a communication according to the standard of Bluetooth, respectively." *Id*., [0067]. Therefore, a POSITA would have understood that the mobile phone 40 of Hiroishi is a short-range wireless-enabled (i.e., Bluetooth enabled) cellular phone. A POSITA would have recognized that Bluetooth was a short-ranged wireless communication protocol. *See* BD-1019, 87 ("Bluetooth wireless technology is a short-range communications system intended to replace the cable(s) connecting portable and/or fixed electronic devices.").

[7.1] a memory device;

850. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [7.1]. In my opinion, Hiroishi-Kahn-Endsley-Bluetooth teaches a memory device. For example, "the mobile phone 40 is configured so as to be mutually connected

by a bus with a CPU (central processing unit) 41 that is responsible for the entire operation of the mobile phone 40; a ROM 42 for recording various control programs, parameters, and so forth; a RAM 43 used as a work area, or the like, at the time of execution of various control programs" Hiroishi [0051].

851. FIG. 3 shows the features of the mobile phone, including a memory device:



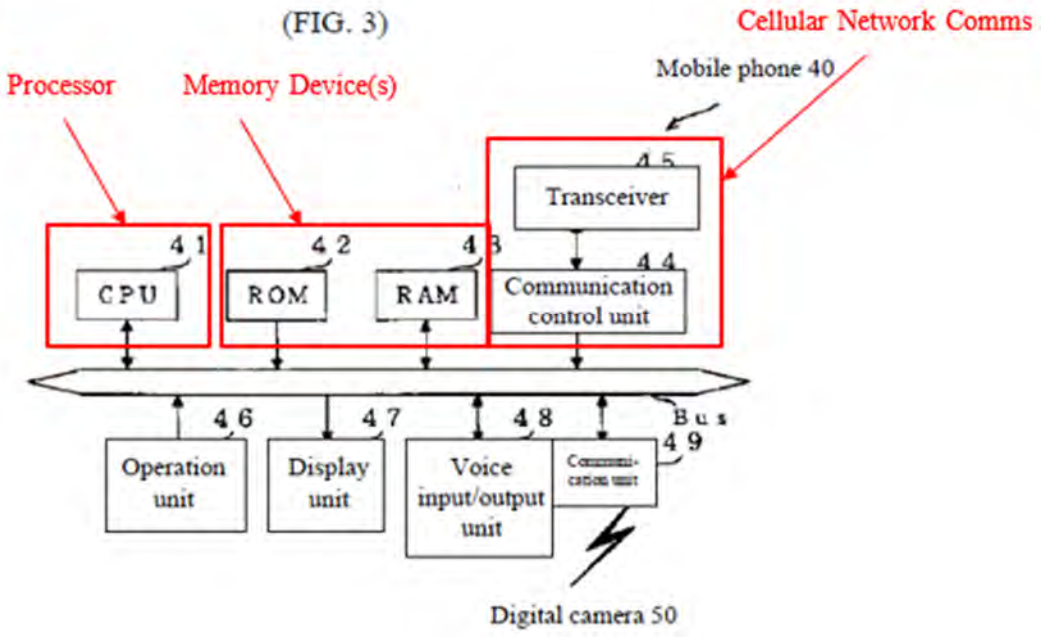
Hiroishi, FIG. 3.

[7.2] a processor coupled to the memory device;

852. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [7.2]. In my opinion, Hiroishi-Kahn-Endsley-Bluetooth teaches a processor coupled to the memory device. For example, "the mobile phone 40 is configured so as to be mutually connected by a bus with a CPU (central processing unit) 41

that is responsible for the entire operation of the mobile phone 40; a ROM 42 for recording various control programs, parameters, and so forth; a RAM 43 used as a work area, or the like, at the time of execution of various control programs" Hiroishi [0051].

853. FIG. 3 shows the features of the mobile phone, including a processor coupled to the memory device:

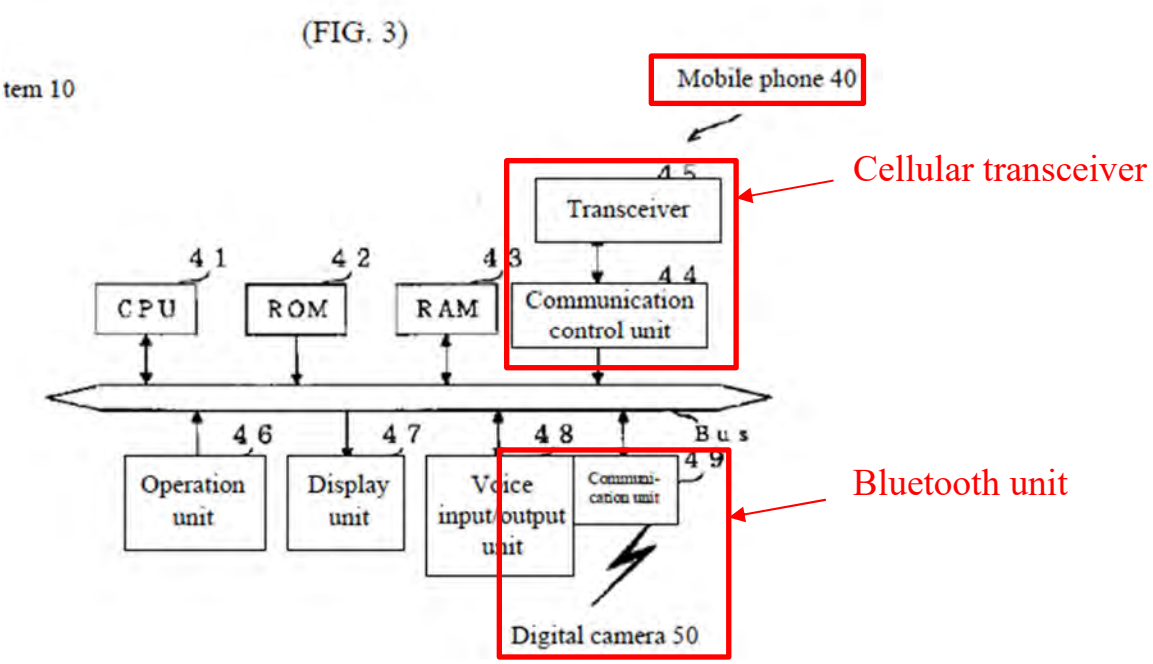


Hiroishi, FIG. 3.

[7.3] a cellular network communication device configured to connect to internet via a cellular data network;

854. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [7.3]. In my opinion, Hiroishi-Kahn-Endsley-Bluetooth teaches a cellular network communication device configured to connect to internet via a cellular data network. FIG. 3 shows the features of the mobile phone, including a cellular

network communication device (44 and 45):



Hiroishi, FIG. 3.

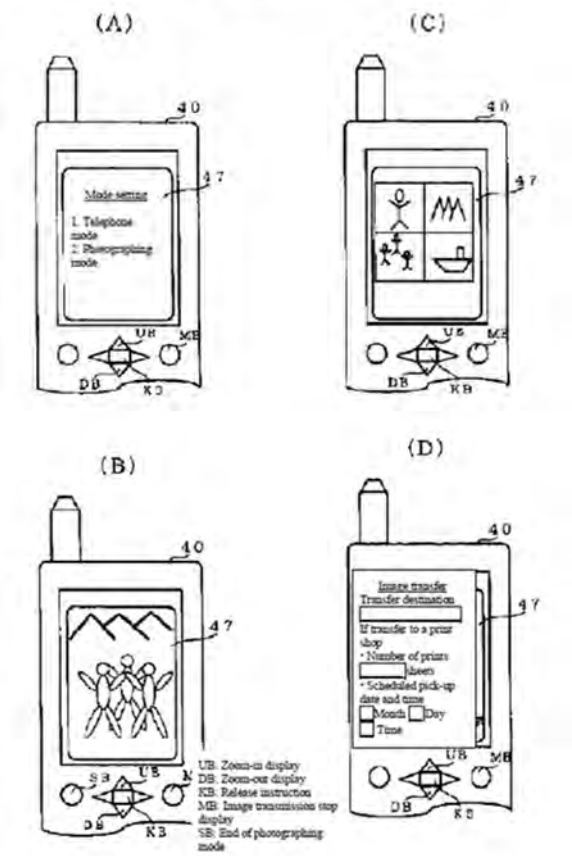
855. Hiroishi teaches that the mobile phone 40 includes a "communication control unit 44 is connected to a transceiver 45 for modulating carrier waves by the voice data for transmission or packet information under the control of the communication control unit 44, using these as a radio signal for the transmission from an antenna, and demodulating the radio signal received from the antenna to restore the voice data or packet information." Hiroishi, [0052].

856. A POSITA would have recognized that the communication control unit and transceiver in Hiroishi were for communicating across a cellular network,

thereby making the mobile phone 40 a cellular phone. *See, e.g.*, Hiroishi, [0052], FIGS. 2-3; see also *id*., [0048] (describing telephone networks 16A and 16B as including a "Personal Digital Cellular" network).

857. For example, as shown in FIGS. 7A-D, Hiroishi teaches a cellular phone that includes a user interface for interacting with digital images received from a digital camera over a Bluetooth connection. The UI permits the user to control the operation of the digital camera, the selection of images, the transmission of thumbnails, and the transmission of selected images to a remote server using the Internet.

(FIG. 7)



Hiroishi, FIGs. 7A-D.

858. Hiroishi teaches a CPU that "is responsible for the entire operation of the mobile phone 40." [0051]. Hiroishi also teaches a ROM 42 for recording various control programs, parameters, and so forth; a RAM 43 used as a work area, or the like, at the time of execution of various control programs." *Id*.

> (0043) As shown in the drawing, the photographing system 10 according to this embodiment is a system wherein various keys provided to **the mobile phone 40** are used to remotely operate the digital camera 50 by transmitting various instruction information from the mobile phone 40 to the digital camera 50.

> (0044) When the digital camera 50 receives from the **mobile phone 40** the instruction information for the purpose of transmitting the image information obtained by photographing, the photographing system 10 transmits the image information to the mobile phone 40, and the mobile phone 40 forwards the image information received from the digital camera 50 to a terminal device. In the case of the transfer of the image information from the mobile phone 40 to the terminal device, character information can also be transmitted to the terminal device along with the image information if needed.

Hiroishi, [0043]-[0044].

[7.4] a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled cellular phone and a short-range wireless enabled data capture device,
wherein the short-range wireless enabled data capture device is configured to cryptographically authenticate identity of the short-range wireless enabled cellular phone;

859. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [7.4]. Hiroishi-Kahn-Endsley-Bluetooth teaches a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled cellular phone and a short-range wireless enabled data capture device, wherein the short-range wireless enabled data capture device is configured to cryptographically authenticate identity of the short-range wireless enabled cellular phone.

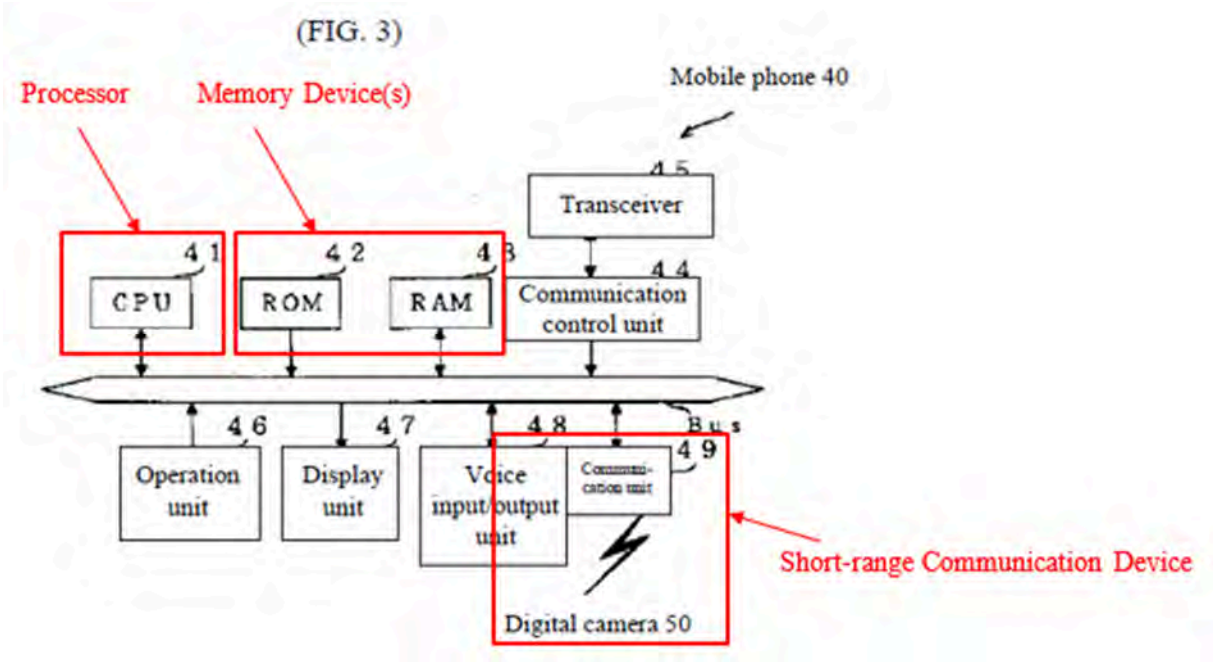
860. This limitation is broken down into constituent steps below:

[7.4.1] a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless

enabled cellular phone and a short-range wireless enabled data capture device,

861. For example, Hiroishi teaches a short-range wireless communication device, which can be a digital camera 50. As described by Hiroishi, "the photographing system 10 according to this embodiment is configured to include a mobile phone 40 and a digital camera 50 configured so as to allow two-way communication, and a terminal device configured so as to allow two-way communication with the mobile phone 40." Hiroishi, [0042].

862. FIG. 3 shows the short-range wireless communication device, which is used to establish the Bluetooth connection with the camera.



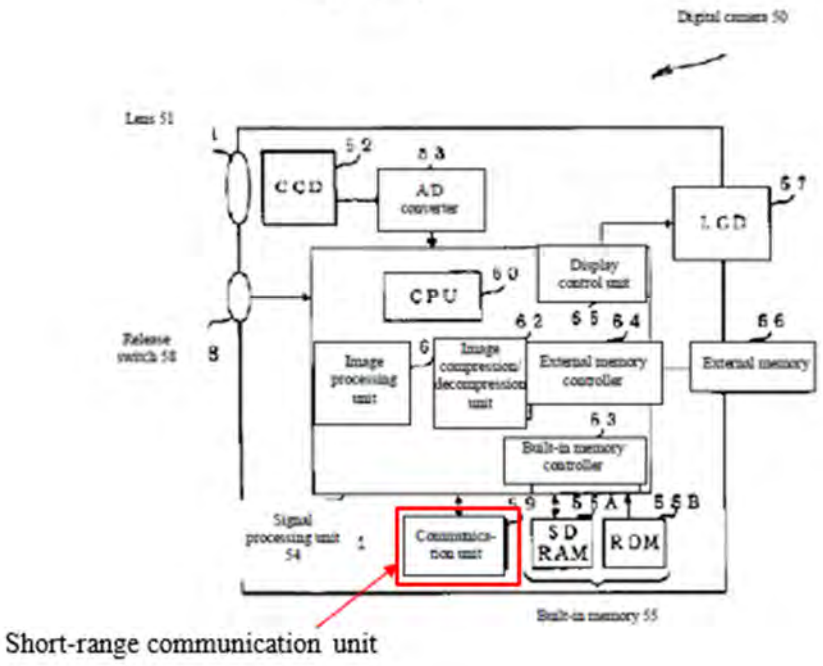
Hiroishi, FIG. 3.

863. As taught by Hiroishi, "a communication unit 49 for carrying out a communication corresponding to a predetermined communication protocol with

the digital camera 50." Hiroishi, [0051]. Hiroishi, [0067] ("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. In this embodiment, the communication unit 49 is built in the mobile phone 40, and the communication unit 59 is built in the digital camera 50.").

864. At FIG. 4, Hiroishi illustrates the features of the digital camera:

(FIG. 4)



Hiroishi, FIG. 4.

865. The digital camera includes "a communication unit 59 for performing communication corresponding to the predetermined communication protocol with the mobile phone 40." Hiroishi, [0058]. Hiroishi teaches a communication unit 49

"for carrying out a communication corresponding to a predetermined communication protocol with the digital camera 50." Hiroishi, [0051]. The communication unit 49 pairs with the communication unit 50 in a manner compliant with Bluetooth protocols.

> The photographing system 10 according to this embodiment is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through **Bluetooth**. Bluetooth is a wireless transfer standard that uses a 2.4 GHz bandwidth and does not require any license to use, and can perform transfer of data signals in the **range within about 10 m**.
>
> 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." Hiroishi, [0066]-[0067].

Hiroishi, [0066]-[0067].

866. A POSITA would have recognized Bluetooth as a short-range communication (i.e., 10 meters). *See, e.g.*, BD-1019, 87 ("Bluetooth wireless technology is a short-range communications system intended to replace the cable(s) connecting portable and/or fixed electronic devices.").

[7.4.2] wherein the short-range wireless enabled data capture device is configured to cryptographically authenticate identity of the short-range wireless enabled cellular phone;

867. As mentioned above, Hiroishi teaches Bluetooth as the communication protocol for communications between the camera and the mobile

phone. *Supra*, [7.4.1]. While a POSITA would recognize that Hiroishi's use of Bluetooth would require pairing the mobile phone with the camera according to Bluetooth standards, Hiroishi does not expressly disclose the camera cryptographically authenticating the identity of the phone. A POSITA would have recognized, however, that cryptographically authenticating the identity of the phone is a required step in pairing the Bluetooth devices using either . *See, e.g.*, BD-1019 , 131 (Secure Simple Pairing), 410, 412, 425 (Pairing).

868. Cryptographic authentication between wireless devices like a digital camera and cellular phone communicatively coupled via Bluetooth was required for Bluetooth pairing at the time of the alleged Critical Date. For example, the Bluetooth Core Specification V2.1 describes two cryptographic authentication processes, the first being LMP Pairing (PIN-code based) and the second being the Secure Simple Pairing (SSP) processes as described in section V.B above. Specifically, the first authentication and pairing process includes the exchange of BD_ADDR, which is a Bluetooth device identifier, along with an initialization key and PIN (which facilitates the claimed cryptographical authentication):

4.2 SECURITY

4.2.1 Authentication

The authentication procedure is based on a challenge-response scheme as described in [Part H] Section 3.2.2 on page 862. The verifier sends an LMP_au_rand PDU that contains a random number (the challenge) to the claimant. The claimant calculates a response, that is a function of this challenge, the claimant's BD_ADDR and a secret key. The response is sent back to the verifier, that checks if the response was correct or not. The response shall be calculated as described in [Part H] Section 6.1 on page 881. A successful calculation of the authentication response requires that two devices share a secret key. This key is created as described in Section 4.2.2 on page 242. Both the master and the slave can be verifiers.

The BD_ADDR is the address of the Bluetooth device, which is a unique identifier. In this way, the cryptographic authentication authenticates the identify of the mobile phone.

4.2.2 Pairing

When two devices do not have a common link key an initialization key (K_{init}) shall be created using either the pairing or Secure Simple Pairing procedures. When pairing is used, K_{init} shall be created based on a PIN, and a random number and a BD_ADDR. K_{init} shall be created as specified in [Part H] Section 6.3 on page 885. When both devices have calculated K_{init} the link key shall be created, and a mutual authentication is performed. The pairing procedure starts with a device sending an LMP_in_rand PDU; this device is referred to as the "initiating LM" or "initiator" in Section 4.2.2.1 on page 242 - Section 4.2.2.5 on page 245. The other device is referred to as the "responding LM" or "responder". The PDUs used in the pairing procedure are:

M/O	PDU	Contents
M	LMP_in_rand	random number
M	LMP_au_rand	random number
M	LMP_sres	authentication response
M	LMP_comb_key	random number
M	LMP_unit_key	key

Table 4.14: Pairing PDUs

All sequences described in Section 4 on page 223, including the mutual authentication after the link key has been created, shall form a single transaction. The transaction ID from the first LMP_in_rand shall be used for all subsequent sequences.

Bluetooth DB-1019, 410-412 (annotated)

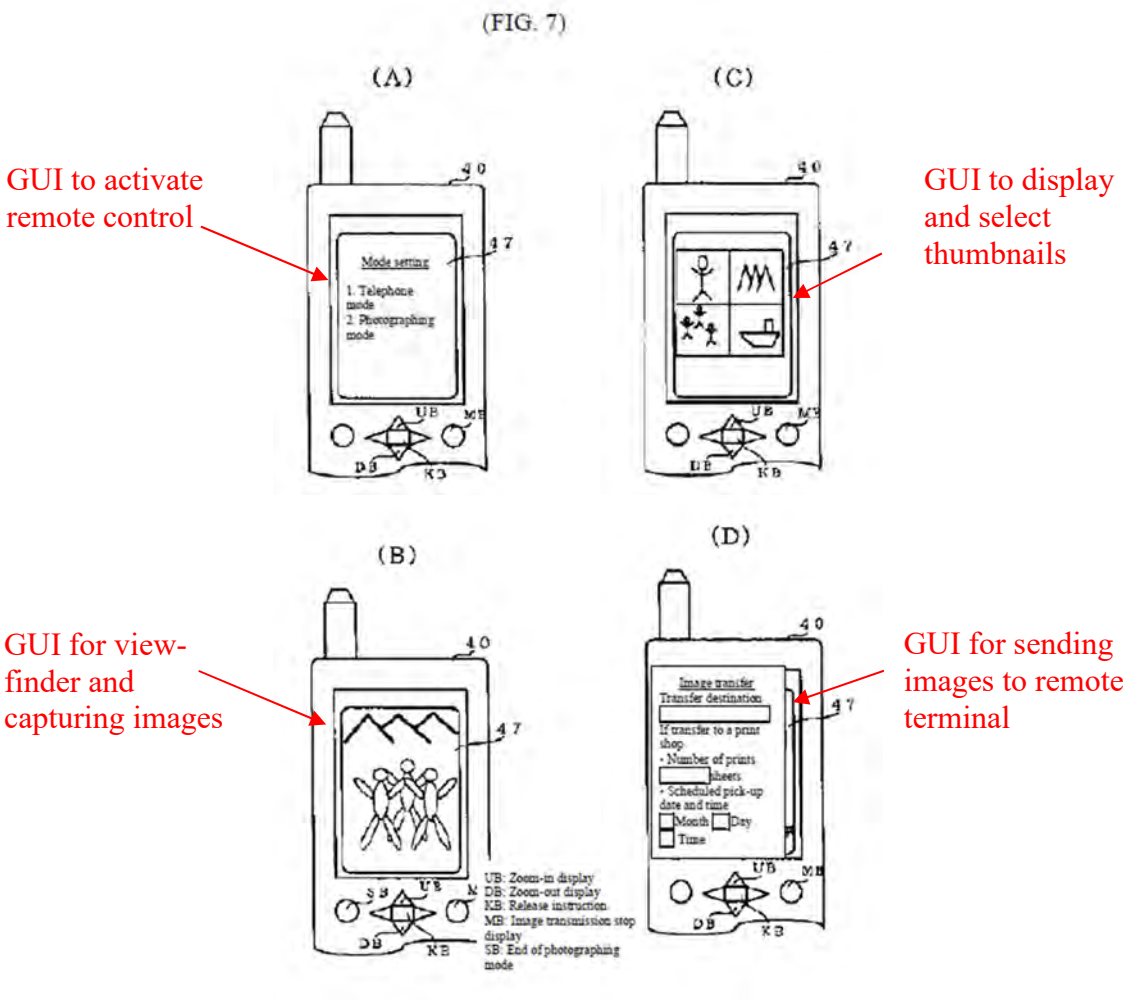
869. As described in the Bluetooth Core Specification, Bluetooth pairing includes the creation of an initialization key (K_{init}) created based on a PIN, a random number, and a BD_ADDR, which is "used to identify a Bluetooth device." *Id*., 89, 410-412. Through the pairing process, using the BD_ADDR of the mobile phone, the camera is configured to cryptographically authenticate the mobile phone.

870. A POSITA would have understood the basic motivation for using cryptographic authentication: to ensure that each device is communicating with its intended recipient and that information is protected from outsiders when transmitted between devices. A POSITA would have found this benefit directly applicable to the system disclosed Hiroishi, because it would have ensured the secure transmission of image files and related data between the two devices. Hiroishi teaches that the camera and phone implement a "predetermined communication protocol" and identifies Bluetooth as the preferred data transmission mechanism, so there would not have been any unexpected result if the camera and phone were configured to cryptographically authenticate each other.

[7.5] a single mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that, when executed by the processor controls the processor to:

871. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious

[7.5]. Hiroishi-Kahn-Endsley-Bluetooth teaches a single mobile client application for the short-range wireless enabled cellular phone comprising executable instructions. For example, Hiroishi teaches a mobile software application for a Bluetooth enabled cellular phone embodied as executable instructions. First, Hiroishi teaches a program on the mobile phone that provides a graphical user interface for controlling the remote operation of the camera, viewing thumbnail images of the images captured, the selection of the images for transmission of the images to a remote terminal, and to provide action settings to the remote terminal concerning the images that are to be uploaded. *See, e.g.*, Hiroishi, [0090]-[0108], FIGS. 7A-D. In FIGS. 7A-D, the GUI is shown for interfacing with the camera for getting photographs and for emailing them to the remote server. For example, as shown in FIGS. 7A-D, Hiroishi teaches a cellular phone that includes a user interface for interacting with digital images received from a digital camera over a Bluetooth connection. The UI permits the user to control the operation of the digital camera, the selection of images, the transmission of thumbnails, and the transmission of selected images to a remote server using the Internet. FIGS. 7A-D are reproduced below:



872. Hiroishi teaches that "the mobile phone 40 is configured so as to be mutually connected by a bus with a CPU (central processing unit) 41 that is responsible for the entire operation of the mobile phone 40; a ROM 42 for **recording various control programs**, parameters, and so forth; a RAM 43 used as a work area, or the like, at the time of **execution of various control programs** . . . ." Hiroishi, [0051]. Further, Hiroishi, [0089] ("FIG. 6 is a flow chart showing the flow of **processing of the mobile phone processing program run by CPU 41 built in the mobile phone 40** when the electric power switch of the mobile phone

40 (not shown) is turned ON, **wherein the program is stored in advance in the predetermined region of ROM 42**.") A POSITA would further understand that because Hiroishi's program is run when the mobile phone's power is turned on, that the mobile phone's application is a **single** application rather than one of multiple mobile client applications chosen when the power is turned on.

873. Hiroishi lists the various instructions that the Bluetooth enabled cellular phone can send to the digital camera over the Bluetooth connection to control the digital camera. *Id*., [0066] . In addition to these instruction information, the instruction information for instructing various operations of the digital camera 50 are also prepared. *Id*., [0068]-[0069].

[7.6] listen for an event notification sent by the short-range wireless enabled data capture device,
wherein the event notification corresponds to new-data and comprises sending a signal by the short-range wireless enabled data capture device to the short-range wireless enabled cellular phone,
wherein the new-data is data acquired by the data capture device after establishing the short-range paired wireless connection with the short-range wireless enabled cellular phone;

874. The Hiroishi-Kahn-Ensley combination renders obvious [7.6]. Hiroishi-Kahn-Ensley teaches that the program on the mobile phone listens for an event notification sent by the short-range wireless enabled data capture device, wherein the event notification corresponds to new-data and comprises sending a signal by the short-range wireless enabled data capture device to the short-range wireless enabled cellular phone, wherein the new-data is data acquired by the data

capture device after establishing the short-range paired wireless connection with the short-range wireless enabled cellular phone.

875. Importantly, a POSITA would have understood that a client application on a mobile phone would run on an application layer, and not on the operating system layer(s) of the mobile phone. By contrast, a POSITA would have recognized that Bluetooth operations, including event notification listening and processing that occur as part of the Bluetooth protocols, occur at the OS and not at the application layer. This distinction is important because of Patent Owner's assertions of infringement of Bluetooth operations by the client application. Here, because a POSITA would have recognized this distinction between application layer and OS layer processing, the prior art discusses application layer programming for listening for and processing for event notifications (i.e., thumbnails).

876. To the extent that the patent owner asserts that a client application performs Bluetooth operations, as opposed to the operating system of the mobile device, Hiroishi's disclosure of Bluetooth would render element [7.6] invalid for analogous reasons. Put simply, Hiroishi teaches Bluetooth communications between the camera and the mobile phone. As an example, Bluetooth includes the inclusion of a TYPE field in the packet payload header indicating the presence of new data; the TYPE field constitutes a signal sent by the camera to the mobile

phone corresponding to the new data (images captured and stored by the camera). *See, e.g.*, BD-1019, 279. The TYPE field of the packet header indicates whether the packet includes a payload. Likewise, during operation, the mobile phone listens for data packets from Bluetooth connected devices, such as the camera in Hiroishi, during predetermined reception (RX) time slots. *See, e.g.*, Bluetooth Core Specification V2.1, 236-240.

877. Hiroishi-Kahn-Endsley-Bluetooth teaches limitation [7.6], which is broken down into constituent parts below:

[7.6.1] listen for an event notification sent by the short-range wireless enabled data capture device, wherein the event notification corresponds to new-data and comprises sending a signal by the short-range wireless enabled data capture device to the short-range wireless enabled cellular phone,

878. Hiroishi teaches that the mobile phone is configured to listen for an event notification from the camera. In Hiroishi, the thumbnails generated after the images are captured and stored on the camera's memory constitute an event notification because each thumbnail represents the event of an image having been captured by the camera. Put differently, the thumbnails are used by the mobile phone user to know what images are captured and stored on the camera after the user sends a release instruction. Note that after the user selects images for transmission to the remote terminal, the camera deletes the images in the camera's memory. *See, e.g.*, Hiroishi, [0084]:

> (0084) In Step 122, a determination is made as to whether the instruction information received in Step 104 is the selected image transmission instruction information; if yes, the process goes to Step 124, wherein a selected image transmission processing is performed, **the selected image transmission processing is that the digital image data corresponding to the image selected by the operator of the mobile phone 40 from a plurality of images shown by the thumbnails transmitted according to the thumbnail transmission instruction information is read from the photographed image data storage area of SDRAM 55A (not shown) is transmitted to the mobile phone 40**, and in the following Step 126, the digital image data read in Step 124 is deleted from the photographed image data storage area of SDRAM 55A, and the process returns to Step 104.

Hiroishi, [0084] (emphasis added).

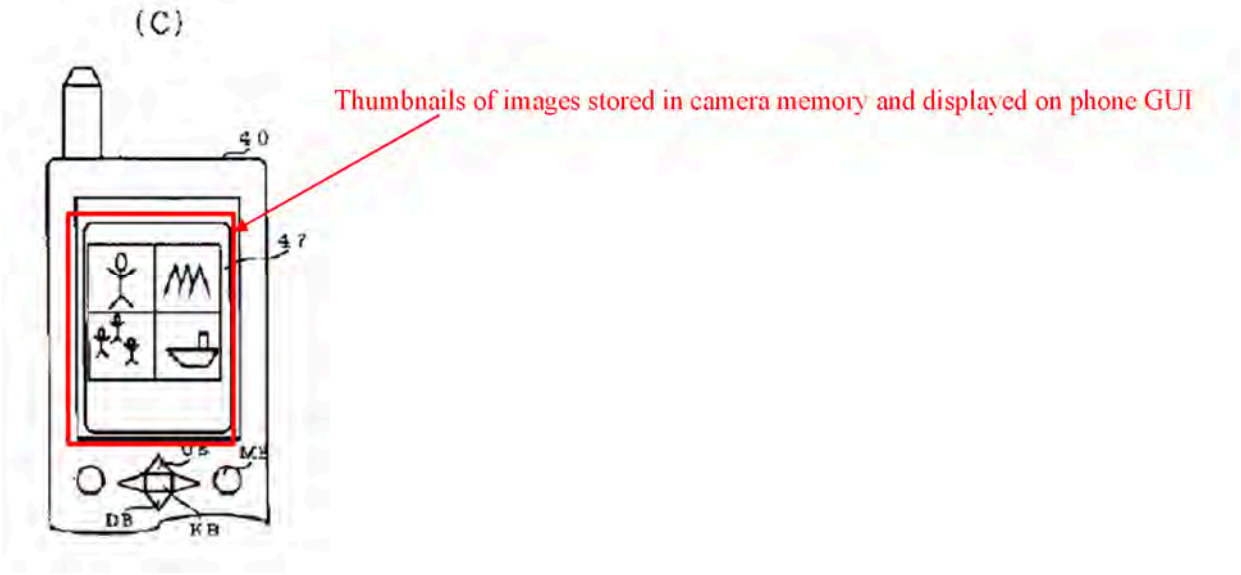
879. Because images are deleted after each image transmission session, the presence of thumbnails in the camera memory means that those thumbnails indicate the presence of new data captured by the camera during that photographing session. Accordingly, the thumbnails represent an event notification, the event being the capturing of one or more new images by the camera.

880. After the mobile phone sends a request for thumbnails instruction to the camera, the phone "waits" for the thumbnail images, which constitutes the phone listening for the event notification signal. *See, e.g.*, [0104].

881. At the cellular phone,

> "when the operator has specified the transmission of the image transmission end instruction information, the process goes to Step 226, wherein the image transmission end instruction information is transmitted via the communication unit 49 to the digital camera 50, and the thumbnail transmission instruction information is subsequently transmitted via the communication unit 49 to the digital camera 50 in Step 228. In response thereto, the digital camera 50 stops the image transmission processing performed in Step 112 of the digital camera processing described above, the thumbnail transmission processing is subsequently performed in Step 120, and the image data for displaying thumbnails is transmitted to the mobile phone 40...
>
> (0104) In the following Step 230, **[the phone] waits** until it receives the image data that can display the thumbnail from the digital camera 50, and in the following Step 232, after a decompression process is performed to the received image data, the thumbnail shown according to the image data is displayed on the display unit 47.
>
> (0105) FIG. 7(C) shows an example of thumbnails displayed on the display unit 47 according to the processing performed in Step 232. As shown in the same drawing, a plurality of images (four images in this drawing) shown according to the digital image data stored in the photographed image data storage area of SDRAM 55A according to the photographing by the digital camera 50 is displayed on the display unit 47 as thumbnails."

Hiroishi, [0102]-[0104] (emphasis added). The one or more thumbnails (event notifications) are shown on the mobile phone's GUI after the thumbnails are received, as shown in FIG. 7C:



Hiroishi, FIG. 7C (annotated)

The thumbnails being sent to the mobile phone constitute the signal representing the event notification. And the phone waiting for the thumbnails constitutes the mobile phone listening for the event notification.

882. Hiroishi teaches that, after sending a request to the digital camera, the cellular phone "waits" for the image data in response. *See, e.g.*, Hiroishi, [0104]. In this way, Hiroishi teaches that the cellular phone "listens" for the event of the arrival of the digital data. Specifically, Hiroishi teaches that the mobile phone sends an instruction to end image transmission, and subsequently waits for the camera to respond with thumbnail pictures. The thumbnail pictures being sent from the camera to the mobile phone constitute the event notification comprising sending a signal from the camera to the cellular phone. (The thumbnails are the

signal.) The thumbnails correspond to the acquired new data (the image captured by the camera when the release instruction is given). The "image data that can display thumbnails is created by performing a predetermined image processing to the digital image data stored in the photographed image data storage area of SDRAM 55A (not shown), a thumbnail transmission processing for transmitting the image data to the mobile phone 40 is performed, and the process returns to Step 104 thereafter." Hiroishi, [0081]-[0082].

[7.6.2] wherein the new-data is data acquired by the data capture device after establishing the short-range paired wireless connection with the short-range wireless enabled cellular phone;

883. As discussed above, Hiroishi teaches that the mobile phone 40 and the digital camera 50 are connected by a Bluetooth connection. Hiroishi, [0066] ("The photographing system 10 according to this embodiment is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth."), [0067] ("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. In this embodiment, the communication unit 49 is built in the mobile phone 40, and the communication unit 59 is built in the digital camera 50."), [0121] ("The case where Bluetooth is applied as a standard of communication for the communication unit 49 and the communication unit 59 has

been described . . . .") See also, id., [0070].

884. After the Bluetooth connection is established, Hiroishi describes that the camera is controlled by the mobile phone using a remote operation. *See, e.g.*, Hiroishi, [0043]. The mobile phone can capture an image remotely using a "release instruction" that the mobile phone transmits to the camera across the Bluetooth connection. *See, e.g.*, *id*., [0066], [0078]-[0079], [0095]-[0096]. As discussed in Hiroishi:

> (0078) In Step 114, a determination is made as to whether the instruction information received in Step 104 is the release instruction information; if yes, the process goes to Step 116, a predetermined image processing is performed to the digital image data input from A/D converter 53, the image recording processing for storing it in the photographed image data storage area (not shown) of SDRAM 55A is subsequently performed, and the process then returns to Step 104.

Hiroishi, [0078] (describing that instructions and images are transmitted to/from+ the communication unit 59, which a POSITA would have recognized was done after the establishment of the Bluetooth connection). A POSITA would have recognized that the data transfer between the digital camera and the mobile phone would occur after the Bluetooth connection had been established.

[7.7] receive the event notification and the new-data from the short-range wireless enabled data capture device;

885. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [7.7]. Hiroishi-Kahn-Endsley-Bluetooth teaches that the mobile phone receives the

event notification and the new-data from the short-range wireless enabled data capture device. As discussed above regarding receiving the thumbnail images (event notification signal). *Supra* [7.6].

886. In addition, Hiroishi teaches receiving image data (new data) from the camera across the Bluetooth connection. Hiroishi, [0107] ("In the following Step 238, [the phone] waits for the reception of the digital image data transmitted from the digital camera 50, and in the following Step 240, a predetermined image transfer screen is displayed on the display unit 47.") Later, Hiroishi describes the mobile phone being able to transfer the images to a remote terminal. *See, e.g.*, Hiroishi, [0108]. A POSITA would have recognized that in order to transmit the images to a remote terminal, the mobile phone must have first received the digital image data (new data) from the camera.

887. A POSITA would have understood that the reception of the Bluetooth compliant packet means that the packet header and the payload are received. The packet header includes a type field, which constitutes the event notification because it indicates to the phone that the packet includes new data. The payload of the packet, of course, includes the new data itself.

888. Thus, a POSITA would have understood that the phone receives the event notification (packet header type field) and the acquired new data (digital image data payload). Note that after the camera sends the images, the images are

deleted from the camera. *See, e.g.*, Hiroishi, [0084], [0106].

[7.8] process the event notification and store the received new-data in the memory device;

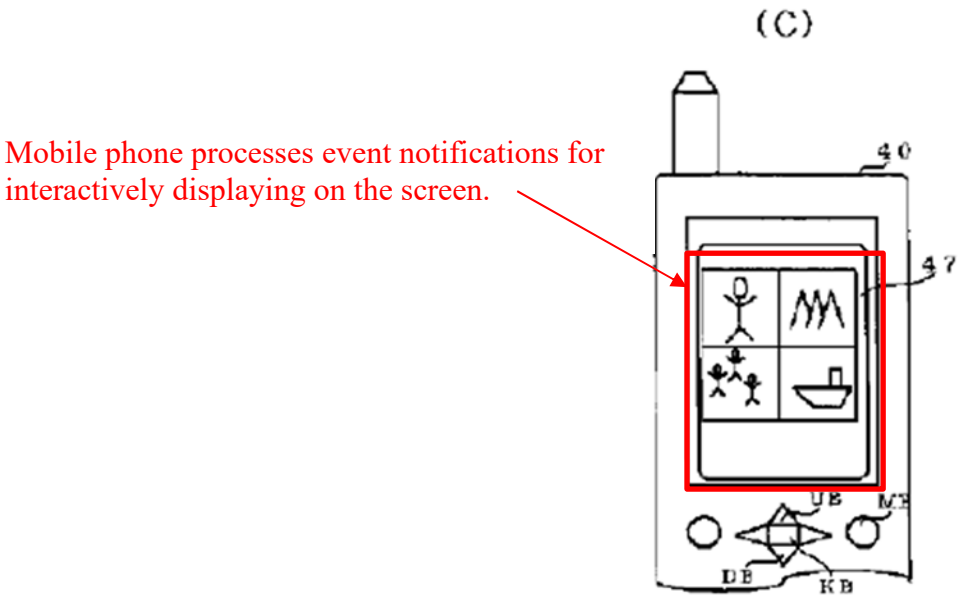
889. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [7.8.]. -Kahn-Endsley teaches processing the event notification and storing the received new-data in the memory device.

890. This limitation is broken down into constituent steps below:

[7.8.1] process the event notification and

891. For example, Hiroishi discloses that the mobile phone receives the thumbnail images from the camera, and the GUI displays the thumbnails on a display that the user can interact with to select new data (images) from the camera storage. Hiroishi, [0081]. A POSITA would have understood that the mobile phone "processes" the event notification by having to display the thumbnails on the screen of the mobile phone in a manner described by Hiroishi.

892. Specifically, Hiroishi describes that the thumbnails are displayed on the mobile phone in a manner that allows multiple thumbnails to be displayed at the same time. *See, e.g.*, Hiroishi, [0104]-[0105], FIG. 7C. FIG. 7C is reproduced below:



Hiroishi, FIG. 7C (annotated).

In addition to displaying the thumbnails, Hiroishi teaches that the thumbnails are interactive such that the user can select a thumbnail as an indication of which image the user wants. *See, e.g.*, Hiroishi, [0105] (describing that the operator using the mobile phone to select a desired image from the thumbnails). A POSITA would have recognized that to organize and display the thumbnails in an interactive manner would mean that the program on the mobile phone would have had to process the thumbnails (the event notifications).

[7.8.2] store the received new-data in the memory device;

893. Hiroishi teaches that a user may access the camera from the phone and select image files to be transmitted to the phone over the Bluetooth connection. Hiroishi does not expressly teach that the phone stores the new media files in

memory device; however, a POSITA reading Hiroishi would have understood that Hiroishi would have had to store the image prior to the image being sent to the remote terminal.

894. First, it is clear that the mobile phone in Hiroishi includes a memory device, which can store images. Specifically, mobile phone 40 includes RAM 43. Hiroishi describes RAM 43 as being "used as a work area, or the like, at the time of execution of various control programs." Hiroishi, [0051]; *see also id*., [0055] (describing SDRAM on the camera for storing digital images); see also *id*., [0013], [0070], [0011]. A POSITA would have recognized that the RAM 43 on the mobile phone would have been used for storing (or, at the very least, temporarily storing) a received image from the camera prior to the mobile phone transmitting the image to the remote terminal. *See, e.g.*, *id*., [0111] (describing the digital image data received is transmitted to the transfer destination); see also *id*., FIG. 6 element 238 ("Received image data?"). That the mobile phone process steps include a determination (or verification) that the mobile phone has received the image data prior to displaying the image transfer screen means that the mobile phone has to store the image data. See also *id.*, [0078], [0084], [0108].

895. Hiroishi teaches that images are received by the mobile phone at one point in time and are transmitted from the mobile at another point in time. Because of this time lag, the mobile phone MUST store the images, at the very least, in a

buffer or other temporary storage device, or in the indicated RAM. This is inherent in Hiroishi.

896. In another example, a POSITA would have recognized that for an image received over a Bluetooth connection, the data representing the image and other data, such as thumbnails and metadata included with the image data, would have to be repackaged as a new packet for transmission across the Personal Digital Cellular network. *See, e.g.*, Hiroishi, [0048].

897. To the extent it is not inherent to store the new data images, a POSITA would have found it obvious to store images in local memory at the mobile phone. A POSITA would have immediately recognized the advantages of storing the storing the new data at the phone after receiving the new data and before sending the new data to the remote server. The known benefits included 1) local storage on the phone for later viewing, 2) rapid access of the images from local storage for transmission, 3) reducing in latency for obtaining images for transmission from, e.g., a remote storage area, 4) reducing in bandwidth or other network resources, 5) facilitating the transition from Bluetooth packet to cellular data packet, etc. The fact that Hiroishi teaches the mobile phone including a RAM 43 means that Hiroishi was already configured to store (at least temporarily) the image data on the mobile phone. A POSITA implementing Hiroishi would have had a reasonable expectation of success storing the new digital image data on the

mobile phone, as was common at the time using RAM.

898. In light of these teachings, a POSITA would have been motivated to use the non-volatile memory on the cellular phone as a predictable location to store new-media files received from the digital camera. As noted above, the benefits of non-volatile memory like RAM were known to those of skill in the art at the time and would have been useful in the cellular phone of Hiroishi. Hiroishi discloses that Mobile phone has two types of memory, 40 ROM 42 and RAM 43, Hiroishi, [0051]. A POSITA would know that a true ROM cannot be written, as it is read only memory. Hiroshi indicates that the ROM has 2 regions, one for the executable program instructions for the CPU 41 and another one for the images, [0088], ("Therefore, the digital camera processing program represents the program of the present invention, and ROM 55B represents the recording medium of the present invention.") so a POSITA would understand that Hiroishi's ROM device is not really a read only memory, but rather a non-volatile memory commonly used at the time of the alleged Critical Date, like a Flash memory (or similar) where some or all sections could be written in circuit (not read only) and furthermore information would not be lost if the power to the mobile phone 40 was lost.

[7.9] store a user authentication credential in the memory device;

899. Hiroishi-Kahn-Endsley-Bluetooth renders obvious [7.9]. In the combination, the single mobile client application (Hiroishi's phone program) stores

a user authentication credential ("network access identifier or NAI (e.g., user cell phone number) and password") in the memory device as taught by Kahn. *Id*.; TTI-1017, [0071], [0064] ("upload program 410 assembles the image data for the images and the corresponding metadata comprising location information and user (identity) information, and then transmits all of that information/data to the image management server, via its communication with the server-side application 440"), [0082] ("the applet retrieves the NAI and password."), [0084] ("the password is stored as part of the applet data"); *see also* TTI-1017, [0071]-[0072], Figs. 5A-F and related descriptions. Indeed, Kahn's upload program 410 is analogous to Hiroishi's phone program.

[7.10] use HTTP to send a user preference to a user data publishing web service over the cellular data network,
wherein the user preference comprises global positioning system information;

900. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [7.10]. Hiroishi-Kahn-Endsley-Bluetooth teaches using HTTP to send a user preference to a user data publishing web service over the cellular data network, wherein the user preference comprises global positioning system information.

901. This limitation is broken down into constituent steps below:

[7.10.1] use HTTP to send a user preference to a user data publishing web service over the cellular data network,

902. In the combination, Hiroishi already teaches that the user of the phone can send the images to a remote server by sending the photos. Hiroishi, [0110]

("When such an image transfer screen is displayed on the display unit 47, an operator enters the information showing the transfer destination of the digital image data received in Step 238 (according to this embodiment, an e-mail (electronic mail) address of the terminal unit of the transfer destination) and the number of sheets to be printed and the scheduled pick-up date and time specifying the terminal unit 20 of a print shop as the transfer destination using the numeric keypad (not shown) or the like, provided on the mobile phone 40 within the corresponding rectangular frame."), [0122]. In addition, Hiroishi already teaches that the mobile phone's program sends the images over a cellular data network. *See, e.g.*, *id*., [0048].

903. Hiroishi is silent, however, as to the protocol used to transmit the images to the user data publishing websites. A POSITA would have found it to be an obvious choice, however, to use HTTP to upload the image(s) from the mobile phone of Hiroishi, in a manner similar to that described in Kahn.

904. For example, Kahn discloses "to communicate with the image management server 330, the host device 320 establishes an Internet connection to the server, for example, using HTTP protocol." Kahn, [0056], FIG. 3; *see also*, *id*., [0055] (describing host device 320 as being a cellular phone). Kahn explains how the upload program responsible for uploading images to the image servers uses HTTP:

[0063] In response to a query from **the upload program 410 (e.g., submitted as an HTTP request), the location API 420 returns GPS information indicating the then-current location (e.g., returned as an HTTP response)**. The GPS information may be converted into decimal values (if not in decimal form already) for indicating longitude and latitude. The upload program 410 also communicates with the camera memory/API 430, so that the upload program 410 can retrieve images from the camera. In this manner, **the upload program 410 is able to invoke transfer of the images from the camera to the host (e.g., cell phone), for uploading to a destination image server.**

[0064] The upload program 410 communicates with the server-side image manager 440, which represents server-side program logic typically implemented at a server (e.g., image management server 330) responsible for image organization (including naming and metadata management). The underlying images themselves will be stored via image servers module 450 (which corresponds to image servers 331, 332, 333) that are in communication with the server-side application 440. The upload program 410 assembles the image data for the images and the corresponding metadata comprising location information and user (identity) information, and then transmits all of that information/data to the image management server, via its communication with the server-side application 440. The file path to an individual image and the metadata/attributes of that image are stored in a corresponding data record in the database 460, which may be implemented using an Oracle database server or the like. Oracle database software is available from Oracle Corporation of Redwood Shores, Calif. **At the completion of upload, image data has been stored at an image server and corresponding metadata information (which now contains the location ID information) has been stored at the database 460.**

Kahn, [0063]-[0064].

[7.10.2] wherein the user preference comprises global positioning system information;

905. In the combination, Hiroishi-Kahn-Endsley-Bluetooth teaches sending global positioning information as a user preference to the user data publishing web service using HTTP. As explained above (supra [7.10.1]), Kahn teaches using HTTP. In addition, Kahn teaches sending GPS information with images using HTTP to the web service. Kahn teaches transmitting a user preference including location information from GPS component. *See, e.g.*, Kahn, [0062]. For example, in Kahn, when "a user wishes to upload images to the user's account on an image server," an "upload program 410 is also invoked." *Id*. The upload program 410 "communicates with the location API 420… that provides an API to the GPS module (e.g., for embodiment having a GPS module embedded within the host/cell phone device)." *Id*. Kahn teaches that the "upload program 410 assembles the image data for the images and the corresponding metadata comprising location information and user (identity) information, and then transmits all of that information/data to the image management Server, via its communication with the server-side application 440." *Id*., [0064].

906. Because Kahn teaches sending the images with the metadata, and Kahn teaches sending images using HTTP, a POSITA would have understood that the metadata, including the global positioning information, was sent to the image servers using HTTP. *See also*, Kahn, [0098].

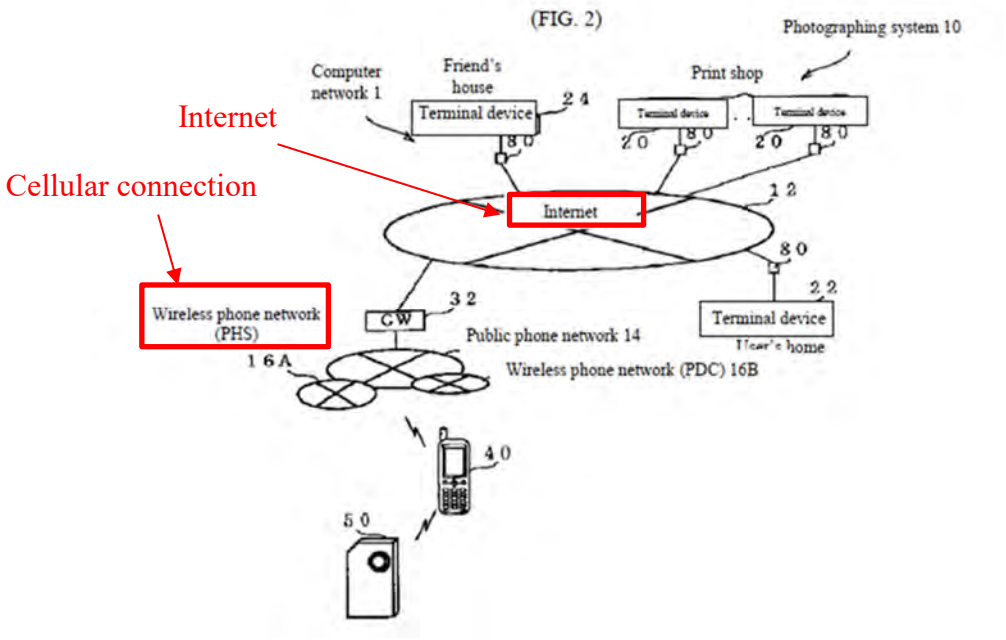
[7.11] further use the HTTP to upload the received new-data and the user authentication credential to the user data publishing web service over the cellular data,
wherein the upload is based on a timer setting on the single mobile client application, and wherein the timer setting is no wait automatic or wait X minutes automatic; and

907. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [7.11.]. Hiroishi-Kahn-Endsley-Bluetooth teaches further use the HTTP to upload the received new-data and the user authentication credential to the user data publishing web service over the cellular data, wherein the upload is based on a timer setting on the single mobile client application, and wherein the timer setting is no wait automatic or wait X minutes automatic.

908. This limitation is broken down into constituent steps below:

[7.11.1] use the HTTP to upload the received new-data and the user authentication credential to the user data publishing web service over the cellular data,

909. As discussed above, Hiroishi establishes that the mobile phone can transfer images to one or more remote terminals across the Internet using a wireless cellular network. *See, e.g.*, Hiroishi, [0047]-[0048], FIG. 2:



Hiroishi, FIG. 2 (annotated)

910. While Hiroishi is silent as to the protocols for transmitting the images to the remote server across the Internet using the cellular network, a POSITA would have found it obvious to use HTTP to do so, in a manner similar to Kahn. Kahn discloses that, "to communicate with the image management server 330, the host device 320 establishes an Internet connection to the server, for example, using HTTP protocol." Kahn, [0056].

911. Kahn also teaches "transmitting the images from the imaging device to a corresponding user account on a Web server." Kahn, Claim 12. "The images are ultimately uploaded to a corresponding user account at the image management

server 330. In the currently preferred embodiment, the 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." Kahn, [0057].

[7.11.2] wherein the upload is based on a timer setting on the single mobile client application, and wherein the timer setting is no wait automatic or wait X minutes automatic; and

912. Hiroishi-Kahn-Endsley-Bluetooth teaches that the upload [of images] is based on a timer setting on the single mobile client application, and wherein the timer setting is no wait automatic or wait X minutes automatic. For example, in the combination, Endsley teaches automatically uploading images to a remote location using a timer setting. Specifically, Endsley teaches that "the communication device 20 may wait to initiate data transfer until a predetermined time." Endsley, [0055]. That predetermined time can be "when transmission rates are low or use of the transmission network by the consumer is unlikely." *Id*. Other examples of a preferred time include "lowest transmission rates, volume of data being received at the service provider, or unlikely utilization of the transmission network by the consumer." *Id*. "The communication device 20 may also monitor consumer usage of the transmission network and choose transmission times (periods) which are unlikely to interfere with other consumer usage." *Id*.

913. Endsley teaches the use of a clock that is used for "transmission of

digital data . . . at certain designated time periods." Endsley, [0048]. "For example, data may be transmitted only at off hours, (e.g. during the middle of the night) when transmission rates are low and there is a relatively lower chance of disruption to the user in the use of the network system." *Id*. Endsley makes it clear, however, that "the communication device 20 may be programmed for allowing transmission during at any desired time period." *Id*.

914. That Endsley teaches that the clock can be used to automatically transmit the images at any desired time period satisfies the claim limitation of a wait x minutes automatic or no wait automatic. A POSITA would have recognized that the transmission of the data based on a timer setting was automatic by contrasting Endsley's disclosure that, in the alternative to using the time period, "the customer may press button 38 to initiate data transfer." for no wait. Endsley, [0055]. ("Alternatively, the communication device 20 may wait to initiate data transfer until a predetermined time . . . .").

[7.12] provide a touch based graphical user interface for the received new-data.

915. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [7.12]. In my opinion, Hiroishi-Kahn-Endsley-Bluetooth teaches providing a touch based graphical user interface for the received new-data. For example, Kahn discloses a mobile phone involving touch based GUI, Kahn, [0045] ("the digital camera 100 would occasionally be connected to a local host device, such as a

cellular phone or a Palm PDA device (available from Palm, Inc. of Santa Clara, Calif.) with wireless connectivity (e.g., Palm i705).") Additionally, Shiigi confirms that the Palm i705 has a touch based graphical user interface.[2] Thus, a POSITA would have recognized that Palm i705 comprises touch based GUI.

[2] Shiigi discloses "The handwriting or handdrawing input device can be a touch screen", TTU-1029, [0025]. Shiigi also teaches that the "handwritten input can be entered with a touch pen". Id. [0089]. Further, an example Shiigi gives for the touch screen device is "Palm's announced i705 wireless device". Id. [0091].

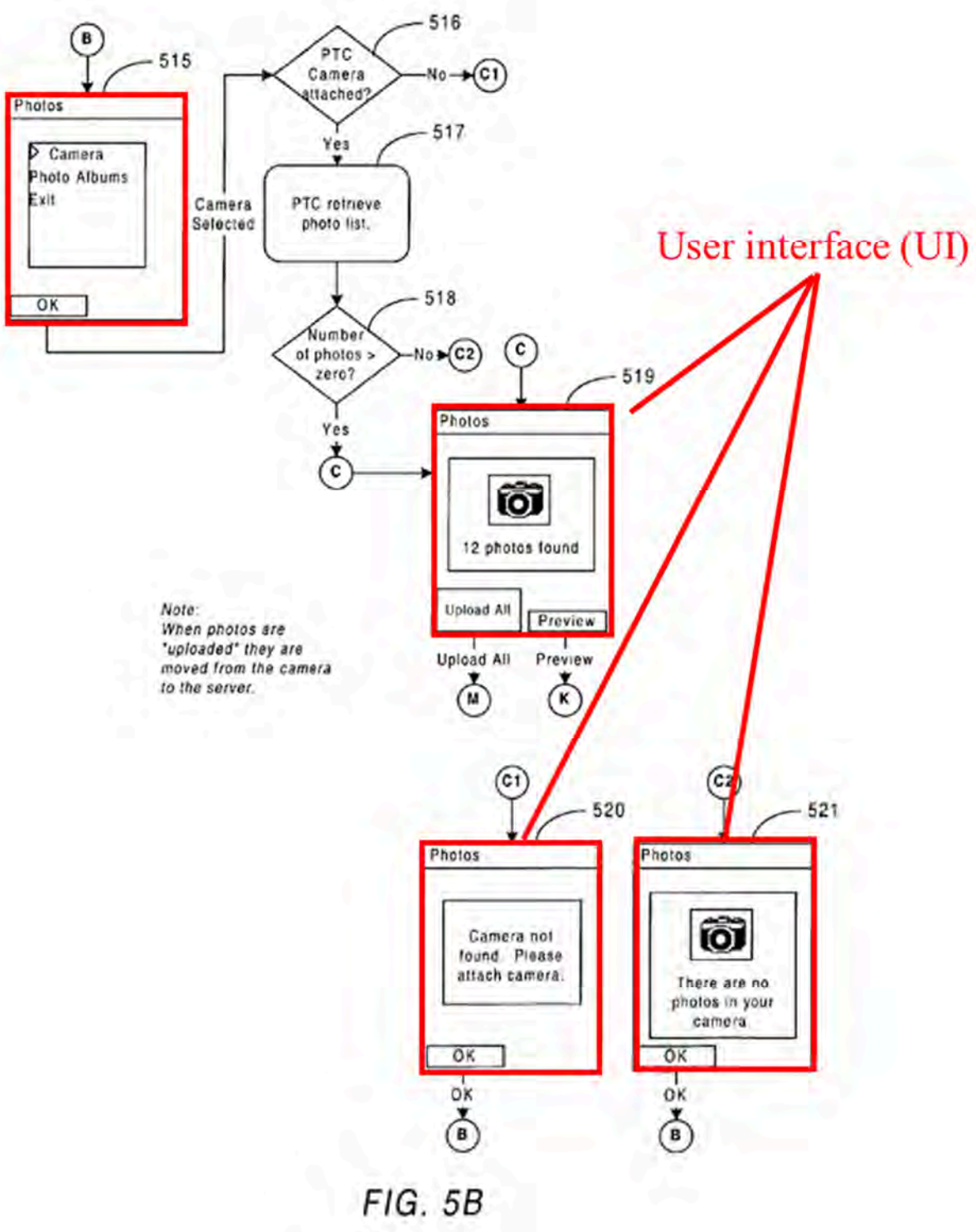


FIG. 5B

Kahn, FIG. 5B (annotated).

916. Based on the examples provided, a POSITA would have understood

that Kahn discloses mobile software application provides a touch based GUI for the received new-data.

917. In an alternative interpretation of the term "touch-based GUI," Hiroishi so teaches. Hiroishi teaches a GUI on the mobile phone that facilitates user interaction using buttons, thereby making Hiroishi's GUI a touch-based GUI. For example, in Hiroishi, the operator presses certain keys for certain commands. *See, e.g.*, Hiroishi, [0090], [0095]-[0100], FIGS. 7A-D. The operation has to touch the buttons to interact with the various images or words or fields presented by the GUI. Therefore, under one interpretation of touch-based GUI, Hiroishi so teaches.

[8] The short-range wireless enabled cellular phone of claim 7, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

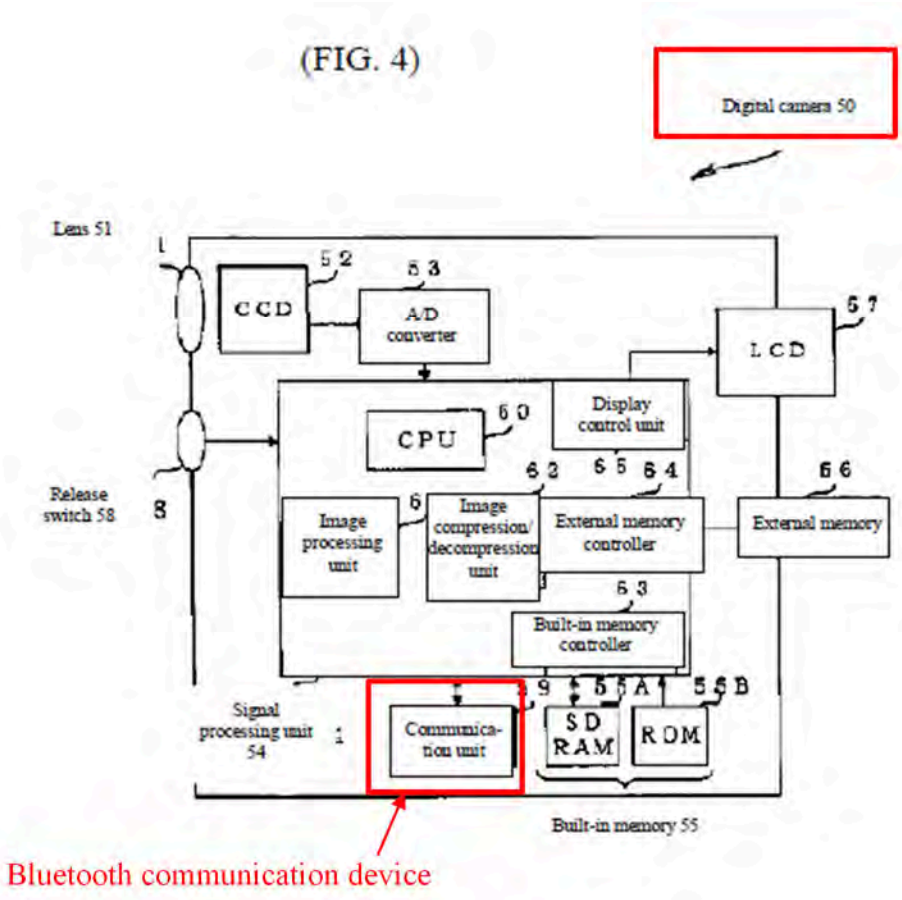
918. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [8]. Hiroishi-Kahn-Endsley-Bluetooth teaches the short-range paired wireless connection is a Bluetooth pairing. *See, e.g.*, Hiroishi, [0066]-[0067], supra [7.P]-[7.4]

Claim 1

[1.P] A short-range wireless enabled data capture device, comprising:

919. To the extent the preamble is limiting, the Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.P]. Hiroishi-Kahn-Endsley-Bluetooth teaches a short-range wireless enabled data capture device (the digital camera of

Hiroishi). For example, Hiroishi teaches a digital camera that has a built-in communication unit for short range communications.

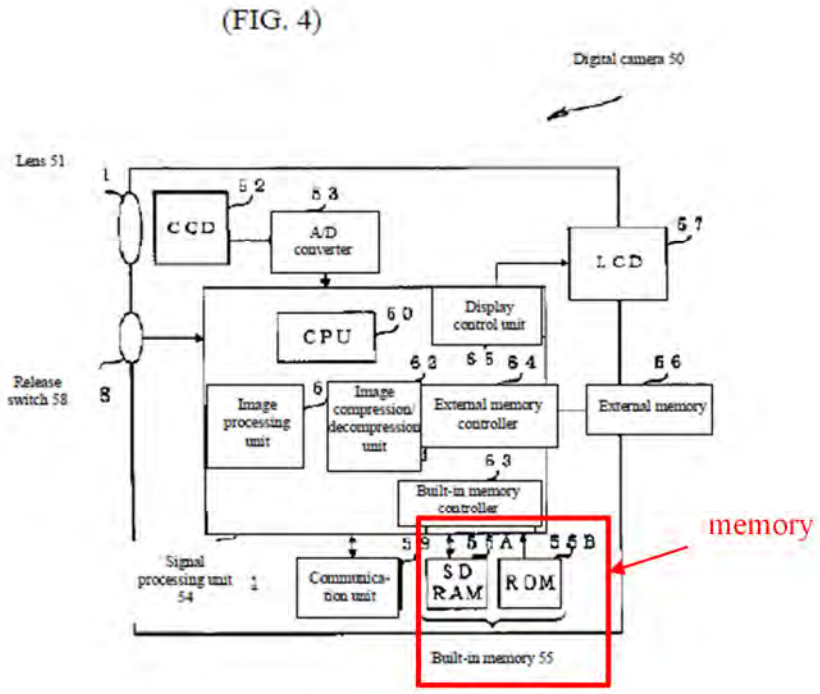


Hiroishi, FIG. 4 (annotated).

920. Hiroishi describes the communication unit 59 as allowing Bluetooth communication between the digital camera and the mobile phone. *See, e.g.*, Hiroishi, [0066]-[0067]. A POSITA would have recognized that Bluetooth was a short-range wireless communication technology. *See, e.g.*, Bluetooth Core Specification V2.1, 87.

[1.1] a memory device;

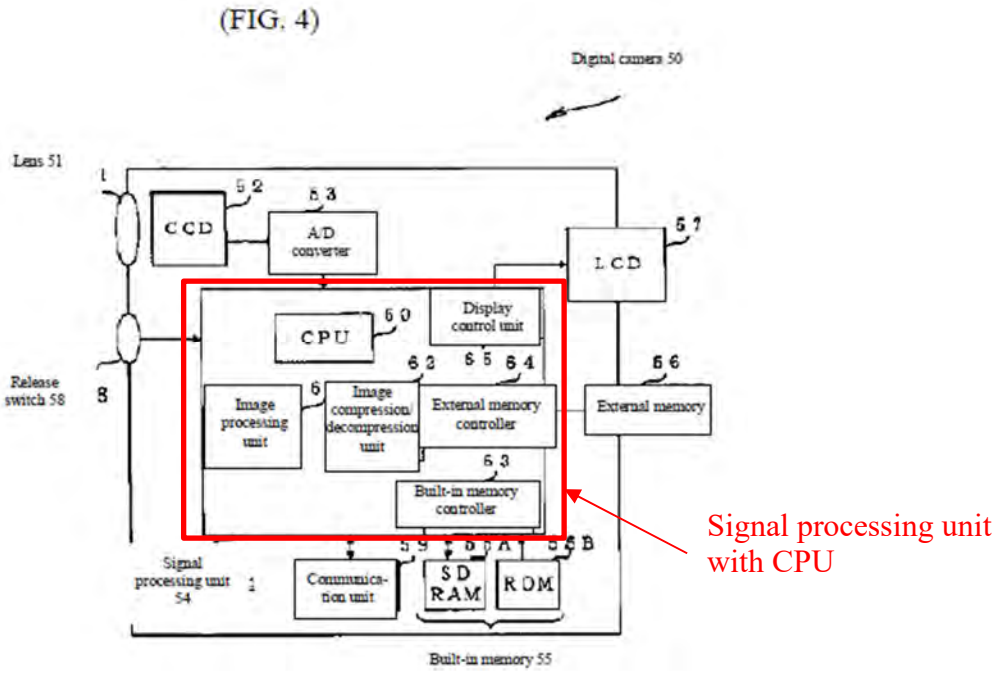
921. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.1]. Hiroishi-Kahn-Endsley-Bluetooth teaches that the camera includes a memory device. For example, Hiroishi teaches that the camera has a memory device:



Hiroishi, FIG. 4 (annotated).

[1.2] a processor coupled to the memory device;

922. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.2]. Hiroishi-Kahn-Endsley-Bluetooth teaches a processor coupled to the memory device. For example, Hiroishi teaches that the camera has a processor coupled to the memory device.

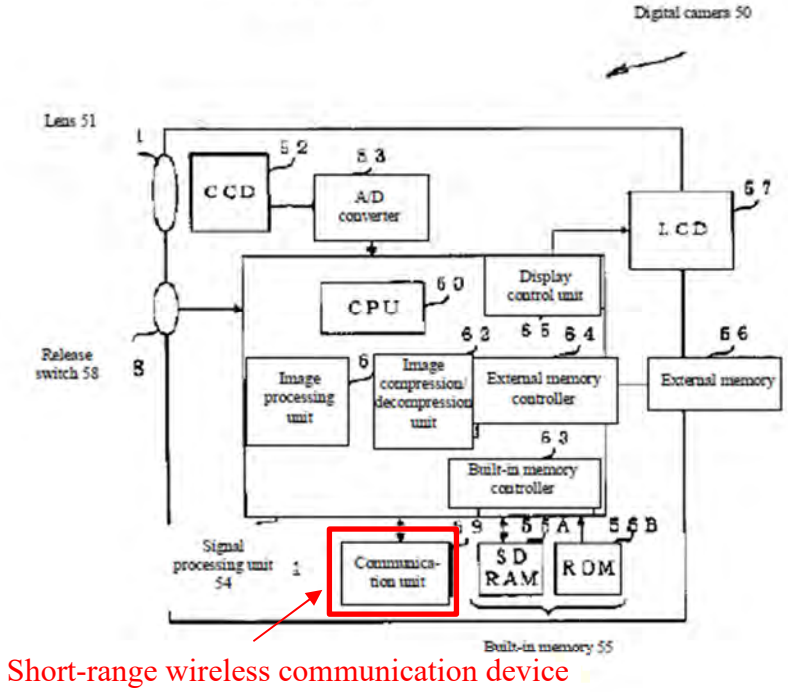


Hiroishi, FIG. 4 (annotated).

[1.3.1] a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone,

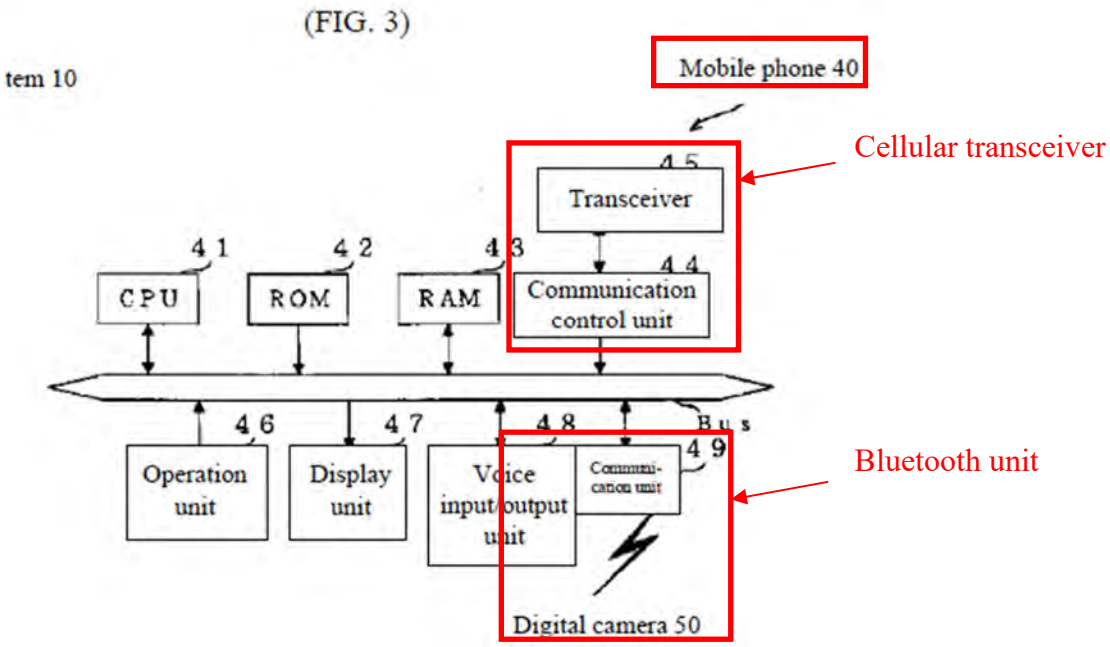
923. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.3.1]. For example, in the combination, Hiroishi teaches that the digital camera 50 includes "a communication unit 59 for performing communication corresponding to the predetermined communication protocol with the mobile phone 40." Hiroishi, [0058] (emphasis added). FIG. 4 illustrates the communication unit 59.

(FIG. 4)



Hiroishi, FIG. 4 (annotated).

The communication unit 59 of the digital camera 50 is "configured so as to allow a communication according to the standard of Bluetooth." *Id.*, [0067]. FIG. 3 shows the Bluetooth communication unit 49 on the cellular phone:



TTI-1011, FIG. 3 (annotated)

A POSITA would have known that Bluetooth was a short-range wireless communication technology. *See, e.g.*, Bluetooth Core Specification V2.1, 87.

[1.3.2] wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled data capture device cryptographically authenticating identity of the short-range wireless enabled cellular phone;

924. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.3.2]. In the combination, Hiroishi teaches that the camera and the mobile phone are connected via Bluetooth, and that various operations occur while the Bluetooth connection is established, including capturing an image and other remote operations. A POSITA would have understood, therefore, that the camera and the

mobile phone in Hiroishi were "paired." While Hiroishi does not expressly disclose the camera cryptographically authenticating the identity of the phone, a POSITA would have known that cryptographically authenticating the identity of the mobile phone was a required part of pairing the camera with the mobile phone. *See, e.g.*, Bluetooth Core Specification V2.1, 410-412.

925. Cryptographic authentication between wireless devices like a digital camera and cellular phone communicatively coupled via Bluetooth was routine at the time of the invention. For example, the Bluetooth Specification (TTI-1019) describes authentication procedures. Specifically, the pairing process includes the exchange of BD_ADDR, which is a Bluetooth device identifier, along with an initialization key and PIN:

4.2 SECURITY

4.2.1 Authentication

The authentication procedure is based on a challenge-response scheme as described in [Part H] Section 3.2.2 on page 862. The verifier sends an LMP_au_rand PDU that contains a random number (the challenge) to the claimant. The claimant calculates a response, that is a function of this challenge, the claimant's BD_ADDR and a secret key. The response is sent back to the verifier, that checks if the response was correct or not. The response shall be calculated as described in [Part H] Section 6.1 on page 881. A successful calculation of the authentication response requires that two devices share a secret key. This key is created as described in Section 4.2.2 on page 242. Both the master and the slave can be verifiers.

The BD_ADDR is the address of the Bluetooth device, which is a unique identifier. In this way, the cryptographic authentication authenticates the identify of the mobile phone.

4.2.2 Pairing

When two devices do not have a common link key an initialization key (K_{init}) shall be created using either the pairing or Secure Simple Pairing procedures. When pairing is used, K_{init} shall be created based on a PIN, and a random number and a BD_ADDR. K_{init} shall be created as specified in [Part H] Section 6.3 on page 885. When both devices have calculated K_{init} the link key shall be created, and a mutual authentication is performed. The pairing procedure starts with a device sending an LMP_in_rand PDU; this device is referred to as the "initiating LM" or "initiator" in Section 4.2.2.1 on page 242 - Section 4.2.2.5 on page 245. The other device is referred to as the "responding LM" or "responder". The PDUs used in the pairing procedure are:

M/O	PDU	Contents
M	LMP_in_rand	random number
M	LMP_au_rand	random number
M	LMP_sres	authentication response
M	LMP_comb_key	random number
M	LMP_unit_key	key

Table 4.14: Pairing PDUs

All sequences described in Section 4 on page 223, including the mutual authentication after the link key has been created, shall form a single transaction. The transaction ID from the first LMP_in_rand shall be used for all subsequent sequences.

Bluetooth Core Specification V2.1, 410-412 (annotated).

The BD_ADDR is the address of the Bluetooth device, which is a unique identifier. In this way, the cryptographic authentication authenticates the identity of the mobile phone.

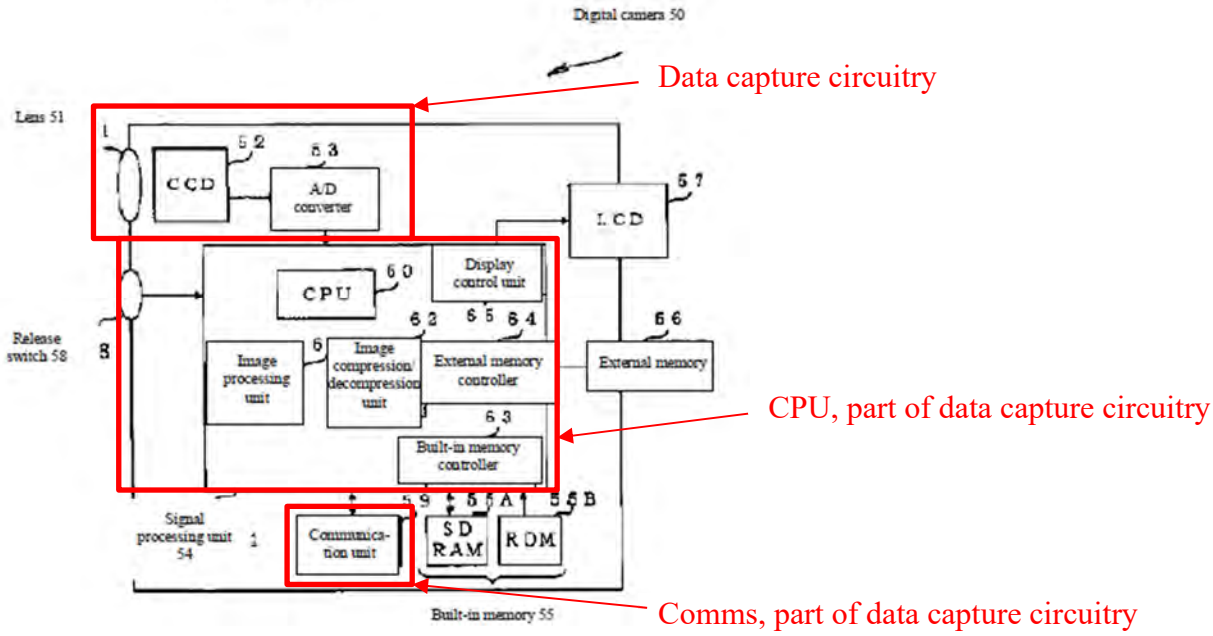
926. As described in the Bluetooth Core Specification, Bluetooth pairing

includes the creation of an initialization key (K_{init}) created based on a PIN, a random number, and a BD_ADDR, which is "used to identify a Bluetooth device." *Id*., 89, 410-412. Through the pairing process, using the BD_ADDR of the mobile phone, the camera is configured to cryptographically authenticate the mobile phone.

[1.4] a data capture circuitry;

927. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.4]. For example, Hiroishi-Kahn-Endsley-Bluetooth teaches that the camera includes data capture circuitry by way of a charge-coupled device (CCD) 52, as well as other image capture elements, such as the analog-to-digital converter (A/D converter) 53 that can be used as part of the image capturing and processing steps.

(FIG. 4)



Hiroishi, FIG. 4 (annotated).

FIG. 4 shows the CCD that is data capture circuitry. The camera includes several other components that can be used in the data capture process. For example, the A/D converter receives electrical signals from the CCD for digitization, which occurs prior to storing the image data.

928. A POSITA would have understood that the release switch is used to take a photo. The release switch functionality is mimicked by the CPU when a release instruction is sent to the camera from the mobile phone. The signal processor is also used as circuitry to capture data when the camera is used in remote control mode. The signal processing circuitry does many functions, like process instructions, process the data, cause the data to be stored or retrieved from storage, and cause the data to be prepared for transmission to the mobile phone.

[1.5] said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;

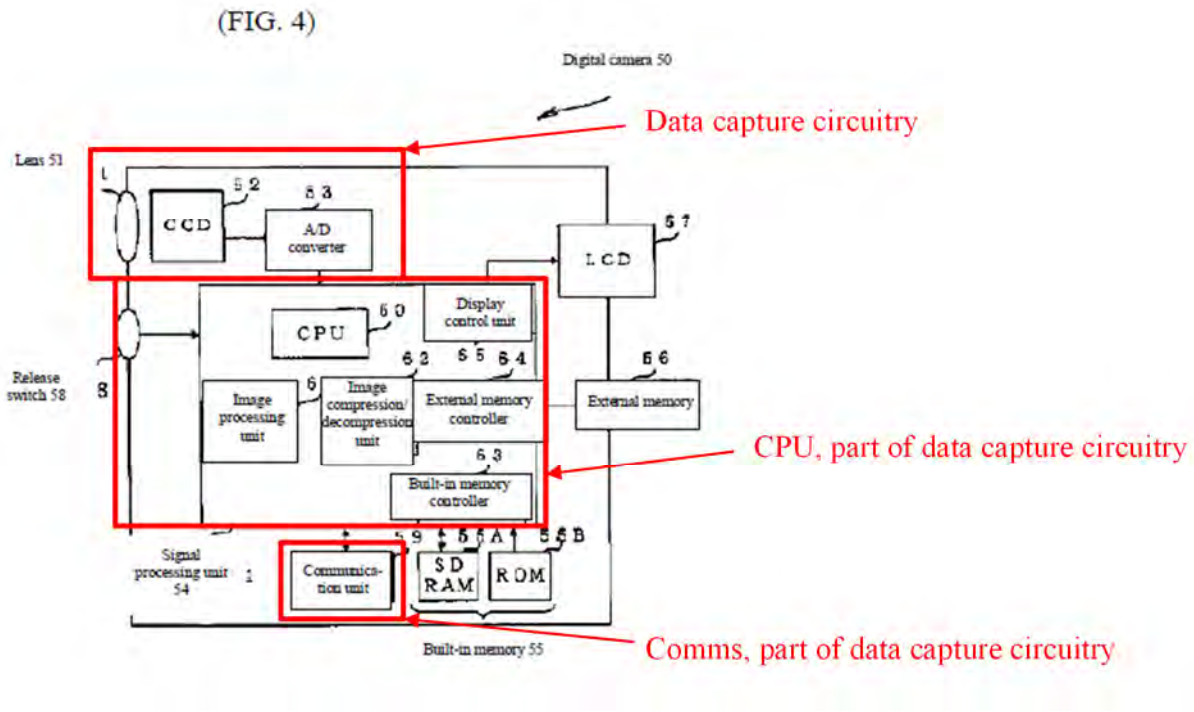
929. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.5]. Hiroishi-Kahn-Endsley-Bluetooth teaches said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled

data capture device and the short-range wireless enabled cellular phone. For example,

930. This limitation is broken down into constituent steps below:

[1.5.1] said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry,

931. In the combination, Hiroishi teaches that the camera's processor is configured to acquire new data.



Hiroishi, FIG. 4 (annotated).

932. FIG. 4 (annotated) shows the CCD that is data capture circuitry. The camera includes several other components that can be used in the data capture process. For example, the A/D converter receives electrical signals from the CCD for digitization, which occurs prior to storing the image data.

933. A POSITA would have understood that the release switch is used by the camera to take a photo. The release switch functionality is mimicked by the CPU when a release instruction is sent to the camera from the mobile phone. *See, e.g.*, Hiroishi, [0078]. The signal processor is also used as circuitry to capture data when the camera is used in remote control mode. *See, e.g.*, *id*., [0078]-[0079]. The signal processing circuitry does many functions, like process instructions, process the data, cause the data to be stored or retrieved from storage, and cause the data to be prepared for transmission to the mobile phone. *Id*.

[1.5.2] wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;

934. Hiroishi teaches that the mobile phone 40 and the digital camera 50 are connected by a Bluetooth connection. Indeed, Hiroishi describes that camera 50 is controlled by the phone 40 using a remote operation. TTI-1011, [0043], [0068]. Specifically, phone 40 transmits across the Bluetooth connection a "release instruction" that causes camera 50 to acquire a new image. *Id.*, [0035], [0066], [0068], [0078]-[0079], [0095]-[0096]. Accordingly, a POSITA would have recognized that the image is acquired after establishing the Bluetooth connection.

935. Hiroshi, [0066]-[0067] ("The photographing system 10 according to this embodiment is configured so as to perform a two-way wireless communication

between the mobile phone 40 and the digital camera 50 through Bluetooth. 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. In this embodiment, the communication unit 49 is built in the mobile phone 40, and the communication unit 59 is built in the digital camera 50.")

936. In this embodiment, the case where Bluetooth is applied as a standard of communication for the communication unit 49 and the communication unit 59 has been described . . . ." Hiroishi, [0121].

937. "[T]he communication unit 59 represents the image information transmission means and the instruction information receiving means of the present invention; . . . the communication unit 49 represents the image information receiving means and the instruction information transmission means of the present invention . . . ." Hiroishi, [0070].

938. "In Step 104, [the camera] waits to receive the instruction information from the mobile phone 40 through the communication unit 59, and in the next step 106, a determination is made as to whether the instruction information received in Step 104 is the image transmission start instruction information; if yes, the process goes to Step 108, the image transmission processing for transmitting to the mobile phone 40 by the communication unit 59 is started after a predetermined image

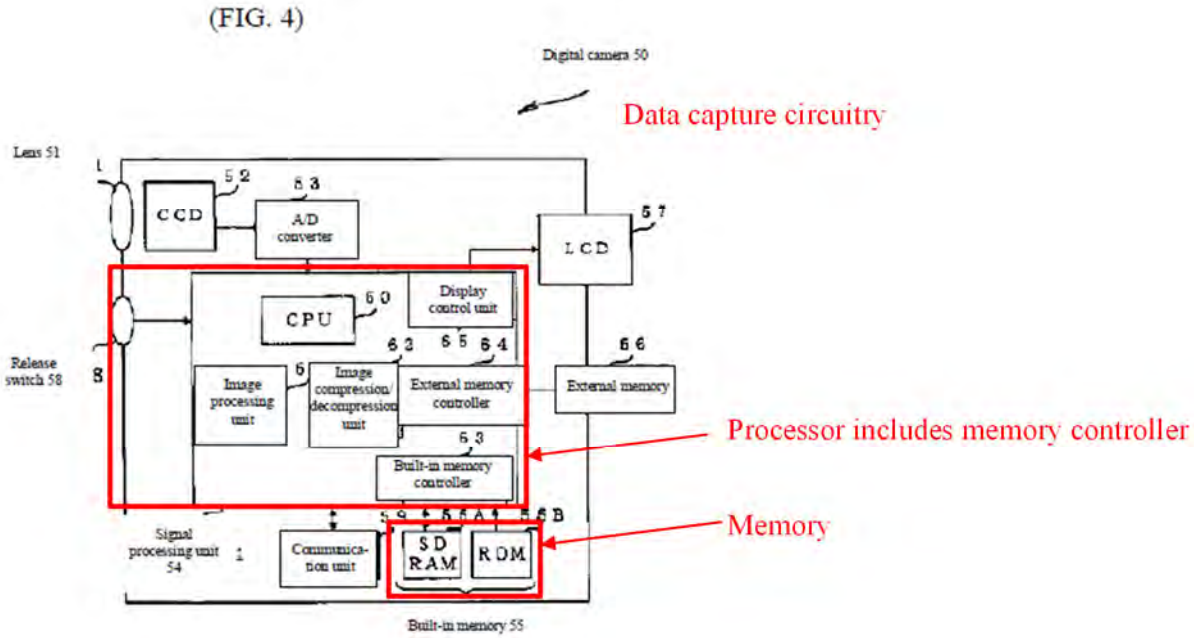
processing has been performed to the digital image data input from A/D converter 53, and the process subsequently returns to step 104." Hiroishi, [0073] (describing that instructions and images are transmitted to/from+ the communication unit 59, which a POSITA would have recognized was done after the establishment of the Bluetooth connection).

939. Hiroishi then discusses all of the instructions transmitted to and images received from the camera. *See, e.g.*, Hiroishi, [0068], [0074]-[0088], *see, e.g.*, *id*., [0091]-[0107].

940. A POSITA would have recognized that the data transfer between the digital camera and the mobile phone would occur after the Bluetooth connection had been established.

[1.6] said processor further configured to store the new-data in the memory device;

941. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.6]. Hiroishi-Kahn-Endsley-Bluetooth teaches said processor further configured to store the new-data in the memory device. *See, e.g.*, TTI-1011, [0078]-[0079], [0105]-[0106] (describing images stored in SDRAM 55A). For example, FIG. 4 shows the processor coupled to the SD RAM (and to the external memory, via memory controller).



Hiroishi, FIG. 4 (annotated showing memory controller part of signal processing unit for storing images in SDRAM).

> (0055) As shown in the drawing, the digital camera 50 is provided with a lens 51 for allowing an object image to form; a CCD (Charge-Coupled Device) 52 for capturing the object image arranged behind the optical axis of the lens 51 and formed by the lens 51, and for outputting it as an analog image signal; an A/D converter 53 for converting the analog image signal output from CCD 52 to digital image data; signal processing unit 54 for performing various signal processing to the digital image data obtained by A/D converter 53; **a built-in memory 55 configured so as to mainly include an SDRAM (Synchronous Dynamic RAM) 55A for temporarily storing the digital image data obtained by photographing** and a ROM 55B for storing in advance various control programs, predetermined parameters, etc.

Hiroishi, [0055] (emphasis added).

> (0078) In Step 114, a determination is made as to whether the instruction information received in Step 104 is the release instruction information; if yes, the process goes to Step 116, a predetermined image processing is performed to the digital image data input from A/D converter 53, the **image recording processing for storing it in the photographed image data storage area (not shown) of SDRAM 55A** is subsequently performed, and the process then returns to Step 104.

Hiroishi, [0078] (emphasis added).

[1.7.1] said processor further configured to send an event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically,

942. Hiroishi-Kahn-Endsley-Bluetooth renders [1.7.1] obvious. A POSITA would find it obvious that a thumbnail is transmitted with additional data that identifies the thumbnail. *Id*. Thus, thumbnail and/or data related to the thumbnail would operate as a notification signal. In addition, this understanding extends beyond thumbnails or image metadata, such as timestamps, to encompass any signal notifying the cell phone of new image data ready for transfer from the camera. Hiroishi's description of Bluetooth-based communication between a camera and a phone, along with the automatic generation and transmission of thumbnails as event notifications, supports this view. Moreover, Kahn's teaching of timestamp inclusion with image data underscores the broader concept of event notifications automatically sent to the mobile phone. Thus, a POSITA would readily recognize the concept of sending a signal to inspire the display of image-

related data, whether thumbnails, timestamps, or any other indication of new data availability for transfer.

943. Further, in the claim, the cellular phone listens for an event notification signal. The signal informs the cellular phone that new data is available. In the combination, there are a variety of signals that would perform the event notification function. For example, Hiroishi sends thumbnails to the cellular phone. Upon receipt of the thumbnails, the cellular phone is notified that the pictures represented by the thumbnails are available. In addition, it would have been obvious to include header information, metadata, or some other information with the thumbnails or in addition to the thumbnails that informs the cellular phone of the nature of the received data—that new photos are available. A person of ordinary skill would have reason to provide an event notification or designate pre-existing data as an event notification so that the cellular phone is made aware that new data is available so that it may then take appropriate actions in response. Because thumbnails provide a straight-forward event notification to the user, a person of ordinary skill would further use the thumbnails or associated metadata identifying the thumbnails as thumbnails as an event notification in the software running on the cellular phone.

944. In the combination, Hiroishi's camera processor is configured to send an event notification (thumbnails) and the acquired new data (image stored in

camera memory) to the mobile phone automatically. Hiroishi's thumbnail transmission instruction is a request for an indication of the new data (images) stored in camera memory. *See, e.g.*, Hiroishi, [0081]-[0082], [0104]-[0105]. In response, the camera sends the thumbnails (event notifications) to the mobile phone, which detects the new data (images) stored in memory through the thumbnails provided to the client application and presented to the user on the GUI. The thumbnails give the client application an indication of the images stored in memory (the new data).

945. In response to the thumbnail request, the camera automatically processes images stored on the camera memory to create the thumbnails, automatically packages the thumbnails for transmission across the Bluetooth link, and automatically transfers the thumbnails to the mobile phone. *See, e.g.*, Hiroishi, [0081]-[0082]; '121 patent, 4:60-67.

946. In Hiroishi, the thumbnails generated after the images are captured and stored on the camera's memory constitute an event notification because each thumbnail represents the event of an image having been captured by the camera. Each thumbnail corresponds to new data acquired, particularly because, after sending the selected images to the user, the camera deletes the images stored in memory. Hiroishi, [0084], [0106]. Thus, the thumbnails represent only the new data, as opposed to old data. The thumbnails are a signal sent to the mobile phone

by the camera. *See, e.g.*, Hiroishi, [0081]-[0082], [0102].

947. In the combination, Hiroishi teaches sending the acquired new data automatically, where the selected images for transmission instruction constitutes the polling request. *See, e.g.*, Hiroishi, [0084], [0104]-[0106]. When the mobile phone sends the selected images for transmission instruction, the camera automatically processes the selected images and automatically transmits the images to the mobile phone across the Bluetooth connection.

948. Note that, in Hiroishi, the program running on the mobile phone receives the event notification (the thumbnail(s)), as required by the claim.

949. 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. TTI-1019, 331-332. Slaves in the active mode listen in the master-to-slave slots for packets.

8.6.1 Polling in the active mode

The master always has full control over the piconet. Due to the TDD scheme, slaves can only communicate with the master and not other slaves. In order to avoid collisions on the ACL logical transport, a slave is only allowed to transmit in the slave-to-master slot when addressed by the LT_ADDR in the packet header in the preceding master-to-slave slot. If the LT_ADDR in the preceding slot does not match, or a valid packet header was not received, the slave shall not transmit.

The master normally attempts to poll a slave's ACL logical transport no less often than once every T_{poll} slots. T_{poll} is set by the Link Manager (see [Part C] Section 4.1.8 on page 234).

The slave's ACL logical transport may be polled with any packet type except for FHS and ID. For example, polling during SCO may use HV packets, since the slave may respond to an HV packet with a DM1 packet (see Section 8.6.2 on page 162).

TTI-1019, 332.

In fact, the Bluetooth Core Specification defines a POLL type data packet that "does not have a payload," "requires a confirmation from the recipient," and "can be used by the master…to poll the slaves." TTI-1019, 283.

950. Another example of event notification in the Bluetooth specification is sniff mode. Sniff mode is used to reduce power during an idle asynchronous connection as an alternative to constantly polling.

8.7 SNIFF MODE

In Sniff mode, the duty cycle of the slave's activity in the piconet may be reduced. If a slave is in active mode on an ACL logical transport, it shall listen in every ACL slot to the master traffic, unless that link is being treated as a scatternet link or is absent due to hold mode. With sniff mode, the time slots when a slave is listening are reduced, so the master shall only transmit to a slave in specified time slots. The sniff anchor points are spaced regularly with an interval of T_{sniff}.

TTI-1019, 345.

951. There is a clear process for enabling event listening using sniff mode.

4.5.3.1 Master or slave requests sniff mode

Either the master or the slave may request entry to sniff mode. The process is initiated by sending an LMP_sniff_req PDU containing a set of parameters. The receiving LM shall then decide whether to reject the attempt by sending an LMP_not_accepted PDU, to suggest different parameters by replying with an LMP_sniff_req PDU or to accept the request.

TTI-1019, 457.

952. Also, in Bluetooth, the transmission routine automatically sends data as long as the transmission buffers include data for transmission. *See, e.g.*, TTI-1019, 94 (4.5.1.1 ACL traffic). The Baseband Resource Manager loads new data information, and as long as the Baseband Resource Manager "keeps loading the registers with new information, the Link Controller will automatically transmit the payload." Id. Thus, in Bluetooth, transmissions of payload are done automatically. For these reasons, in addition to others described above, Hiroishi renders this element invalid.

953. To the extent that the Patent Owner points to Bluetooth for

automatically sending the event notification and the data, Hiroishi's teaching of Bluetooth renders element [1.7.1] obvious and invalid. *See, e.g.*, TTI-1019, 264.

954. In the combination, Hiroishi's mobile phone program sends the acquired new data automatically, where the selected images for transmission instruction constitutes the polling request. TTI-1011, [0084], [0104]-[0106]. When the mobile phone sends the selected images for transmission instruction, the camera automatically processes the selected images and automatically transmits the images to the mobile phone across the Bluetooth connection. *Id*.

955. In addition, or in the alternative, the camera sends a timestamp with the image data as taught by Kahn. *Id.*; TTI-1017, [0008], [0060]. According to the '030 patent, which shares the same specification and priority claim as the '121 patent, the event notification can be timestamp attribute inside the data object. *See, e.g.*, TTI-1001, cl.6. Thus, a POSITA would have recognized that a timestamp was an event notification.

[1.7.2]wherein the event notification corresponds to the acquired new-data and comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone,

956. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.7.2]. Supra [7.6.1]. In the combination, the event notification (Hiroishi's thumbnail and/or Kahn's timestamp) corresponds to the acquired new-data (image) and comprises sending a signal (the signal transmitting the thumbnail, the response

to the Bluetooth polling request, and/or the timestamp) to Hiroishi's cellular phone 40. TTI-1011, [0081]-[0084], [0102]; TTI-1017, [0008], [0060]; *supra*, [1.7.1]. Hiroishi's thumbnail correspond to the image because it is a low-resolution version of the image, making it unique to each image. And Kahn's timestamp corresponds to when the image is captured, making it unique to each image. *Id*.; TTI-1017, [0008], [0060].

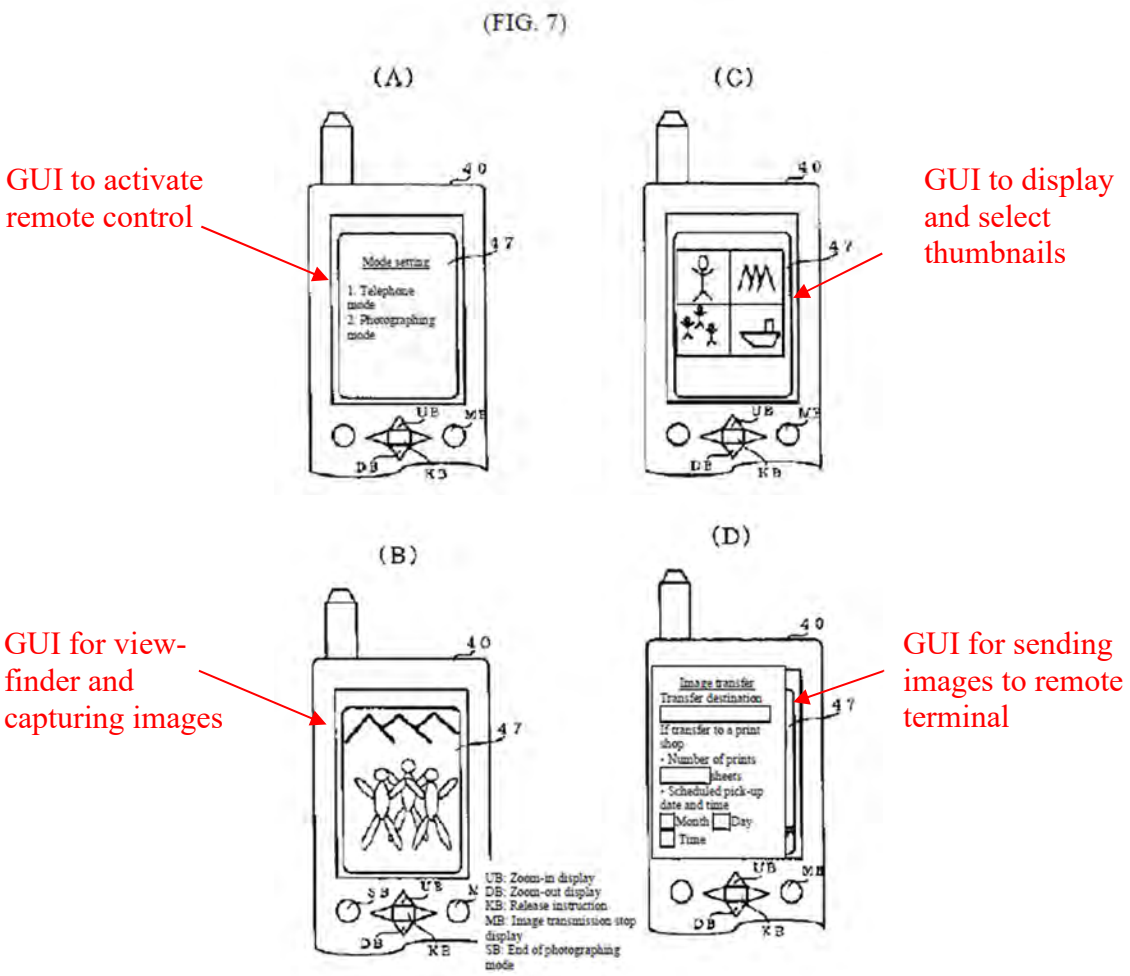
[1.8] wherein the cryptographically authenticated short-range wireless enabled cellular phone is configured to listen to the event notification and receive the new-data over the established short-range paired wireless connection,

957. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.8]. Supra [7.6.1], [7.7]. In the combination, Hiroishi's phone 40 is configured to listen for the event notification (Hiroishi's thumbnail and/or Kahn's timestamp) and to receive the new data (images). *Id*. Hiroishi's phone 40 is configured to listen ("wait") for the thumbnail in response to the thumbnail request. TTI-1011, [0104]. Hiroishi's phone 40, which is a master device, is also configured to listen for responses to Bluetooth polling requests. TTI-1019, 332 (8.6.1 Polling in the active mode). In the combination, responses to Bluetooth polling requests include a thumbnail and/or a timestamp. In the combination, Hiroishi's phone 40 is further configured to receive the new-data (image) over the short-range paired wireless connection (Bluetooth). *Id*.; TTI-1011, [0066]-[0067] [0093], [0107].

[1.9.1]-[1.9.2] wherein a single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the event notification and store the received new-data in a memory device of the cryptographically authenticated short-range wireless enabled cellular phone,

958. Hiroishi-Kahn-Endsley-Bluetooth renders obvious [1.9.1]. In the combination, a single mobile client application (Hiroishi's program running on mobile phone 40) is configured to process the event notification (Hiroishi's thumbnail and/or the response to Hiroishi's Bluetooth polling request for the thumbnail) by displaying a thumbnail in an interactive fashion on the phone's GUI. *Id*.; TTI-1011, [0001], [0089]-[0108], FIGS. 7A-D.

959. Hiroishi's phone 40 includes "a program with which a photographer can simply and reliably captures a self-portrait." TTI-1011, [0001]; *see also id*., [0089] (describing the program being "stored in advance in the predetermined region of ROM 42"), [0068] (describing several instructions that the program on the mobile phone sends to the camera). Hiroishi's program provides a GUI for viewing/selecting thumbnail images. TTI-1011, [0001], [0089]-[0108], FIGS. 7A-D.



Hiroishi, FIGS. 7A-D (annotated).

960. As shown above, Hiroishi discloses that phone 40 receives a thumbnail from camera 50, that the GUI displays the thumbnail, and that that the user can interact with the thumbnail to select new data (images) from the camera storage. TTI-1011, [0001], [0081]-[0082], [0104]-[0105], FIG. 7C. The organization, display, and interaction with the thumbnail involve processing the thumbnail (the event notifications).

961. In the combination, Hiroishi's phone program also processes the

timestamp, as taught by Kahn, when it creates a new packet for transmission of the images to the remote server using HTTP. TTI-1017, [0008], [0056], [0060].

962. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.9.2]. Supra [7.8.1]. In the combination, Hiroishi's phone program is configured to store the received new-data in a memory device (*e.g.*, RAM 43) of Hiroishi's cellular phone 40. *Id.*; TTI-1011, [0051] (RAM 43 is "used as a work area, or the like, at the time of execution of various control programs"); *see also* TTI-1011, [0013], [0070], [0011].

963. Hiroishi does not expressly teach that phone 40 stores images in its memory device. However, a POSITA would have understood and immediately envisaged that Hiroishi necessarily stores the image prior to the image being sent to the remote terminal. Indeed, the processing steps of Hiroishi's phone 40 include a determination (or verification) that the phone received the image data prior to displaying the image transfer screen. *Id.*; TTI-1011, [0078], [0084], [0108]. Hiroishi teaches that images are received by the mobile phone at one point in time and are transmitted from the mobile at another point in time. TTI-1011, [0107]-[0108]. And the data received by Hiroishi's phone 40 over Bluetooth needed to be repackaged for transmission across Hiroishi's Personal Digital Cellular network. TTI-1011, [0048]. Accordingly, a POSITA would have recognized and immediately envisaged that Hiroishi's phone program is configured

to store (either permanently or temporarily, e.g., in RAM 43) the image received from Hiroishi's camera 50 prior to phone 40 transmitting the image to the remote terminal. TTI-1011, [0111] (describing the digital image data received is transmitted to the transfer destination); FIG. 6 element 238 (received image data).

964. To the extent it is not inherent to store the new data images, and a POSITA would not immediately envisage such storage, it would have been obvious for Hiroishi's camera program to store images in the phone's memory. A POSITA would have immediately recognized the advantages of storing the storing the new data at the phone after receiving the new data and before sending the new data to the remote server. *Id*. The known benefits included: (1) local storage on the phone for later viewing; (2) rapid access of the images from local storage for transmission; (3) reducing in latency for obtaining images for transmission from, e.g., a remote storage area; (4) reducing in bandwidth or other network resources; and (5) facilitating the transition from Bluetooth packet to cellular data packet. *Id*.

965. A POSITA implementing Hiroishi would have had a reasonable expectation of success storing the new digital image data on the mobile phone, as was common at the time using RAM. As noted above, Hiroishi's phone 40 already includes RAM 43, which would be used to store (at least temporarily) the image data on the mobile phone. *Id*. And, if necessary, adding additional memory to store one or more images was well within the level of skill in the art. *Id*.

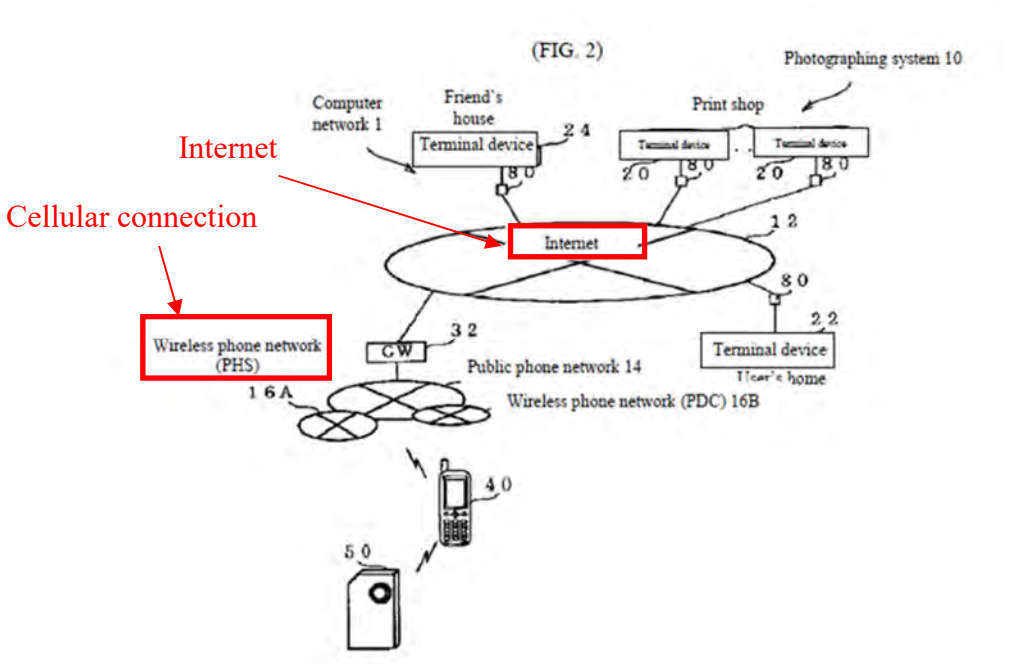
[1.10] wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone stores a user authentication credential in the memory device of the cryptographically authenticated short-range wireless enabled cellular phone,

966. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.10]. Supra [7.8.2]. In the combination, the single mobile client application (Hiroishi's phone program) stores a user authentication credential ("network access identifier or NAI (e.g., user cell phone number) and password") in the memory device as taught by Kahn. *Id*.; TTI-1017, [0064] ("upload program 410 assembles the image data for the images and the corresponding metadata comprising location information and user (identity) information, and then transmits all of that information/data to the image management server, via its communication with the server-side application 440"), [0082] ("the applet retrieves the NAI and password."), [0084] ("the password is stored as part of the applet data"); *see also* TTI-1017, [0071]-[0072], Figs. 5A-F and related descriptions. Indeed, Kahn's upload program 410 is analogous to Hiroishi's phone program.

[1.11] wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to use HTTP to upload the received new-data and the user authentication credential to a user data publishing website over a cellular data network,

967. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.11]. Supra [7.11.1]. In the combination, the single mobile client application (Hiroishi's phone program modified as taught by Kahn) is configured to use HTTP

to upload the received new-data and the user authentication credential to the user data publishing web service over the cellular data. *Id*. Hiroishi's cellular phone 40 transfers images to one or more remote terminals across the Internet using a wireless cellular network. *Id.*; TTI-1011, [0047]-[0048], FIG. 2:



TTI-1011, FIG. 2 (annotated)

In the combination, Hiroishi's phone program uses HTTP to transfer Hiroishi's images and Kahn's authentication credentials to a remote terminal as taught by Kahn. TTI-1030, 967. Kahn discloses that, "to communicate with the image management server 330, the host device [phone] 320 establishes an Internet connection to the server, for example, using HTTP protocol." TTI-1017, [0056]-

[0057]; *see also id*., Claim 12 ("transmitting the images from the imaging device to a corresponding user account on a Web server"). Additionally, Kahn specifies that a "user is given access to photos on the camera or on photo albums (e.g., online photos)." Kahn, [0074]. However, this access is contingent upon the validity of the user credentials. Kahn, [0082], [0084], FIG. 5C (elements 522, 526). For example, Kahn discloses that "the applet [at the cell phone] retrieves the NAI and password" from the cell phone's memory and transmits the login credentials "to the photo site (Web-based server providing image management)" to determine the validity of the user credentials. Kahn, [0082].

[1.12] wherein the upload is based on a timer setting on the single mobile client application, wherein the timer setting is no wait automatic or wait X minutes automatic,

968. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.12]. Supra [7.11.2]. In the combination, Hiroishi's phone program uploads the new-data and the user authentication credential based on a timer setting as taught by Endsley. *Id*. Endsley teaches that "the communication device 20 may wait to initiate data transfer until a predetermined time." TTI-1024, [0055], [0048]. "For example, data may be transmitted only at off hours, (e.g. during the middle of the night)…." *Id*. By waiting until a predetermined time to automatically transmit the images Endsley teaches a timer setting that is "wait x minutes automatic." *Id*. Alternatively, a POSITA would have been motivated to implement the automatic

uploading of images as soon as the camera is connected to the cell phone taught by Kahn. In the combination, Hiroishi's phone program can also upload the new-data and user authentication credentials automatically as taught by Kahn. Kahn, [0064], [0082], [0084], FIG. 5C (elements 522, 526). By transmitting the images automatically, the combination of Kahn and Endsley teaches a timer setting that is "no wait automatic."

[1.13] 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

969. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.13]. Supra [7.10]. In the combination, the single mobile client application (Hiroishi's phone program) is further configured to use HTTP to send a user preference comprising global positioning system information (GPS information as taught by Kahn) to the user data publishing web service over the cellular data network. *Id*.; TTI-1017, [0051], [0058], [0062], [0064], [0098]. As explained in Kahn, "location ID [*i.e*., global positioning system] information may also be conveniently transmitted, either by attaching the information to the image data (e.g., as header information) and/or as a separate (auxiliary) data item." TTI-1017, [0058], [0098].

[1.14] 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.

970. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [1.14]. Supra [7.12]. In the combination, the single mobile client application (Hiroishi's phone program) provides a touch based GUI (Hiroishi's GUI that facilitates user interaction using buttons) for the received new data. *Id.*; TTI-1011, [0090], [0095]-[0100], FIGS. 7A-D. Alternatively, Hiroishi's phone program provides a touch based GUI for the received new-data as taught by Kahn, which, like Hiroishi, discloses an interactive "user interface (UI)" with a screen that displays buttons that change depending on the screen. TTI-1017, FIGS. 5A-E.

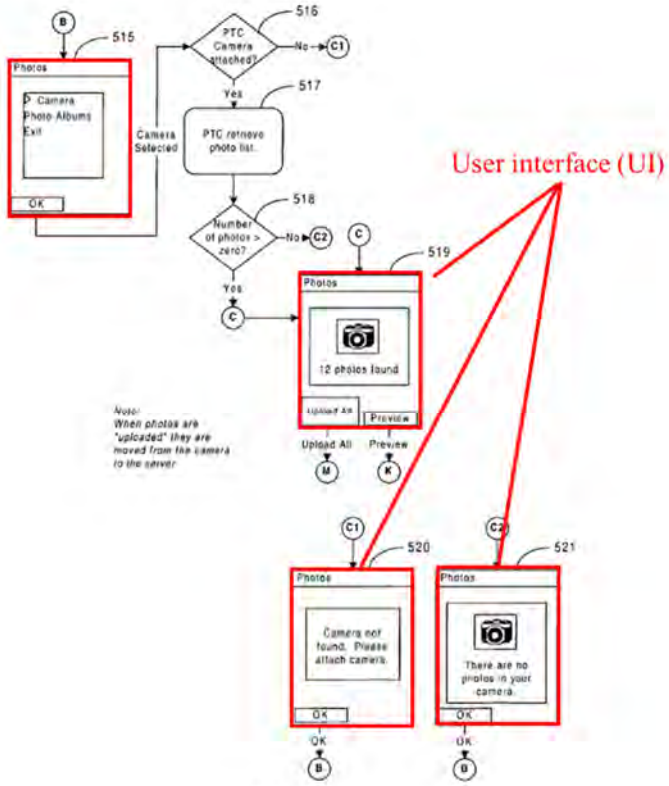


FIG. 5B

TTI-1017, FIG. 5B (annotated).

Notably, Kahn (at [0045]) discloses that the host device can be a PDA, like the Palm i705, which included a touch-screen display. TTI-1029; TTI-1028.

[2] The short-range wireless enabled data capture device of claim 1, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

971. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [2]. Hiroishi-Kahn-Endsley-Bluetooth teaches the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing. Supra [8].

[3] The short-range wireless enabled data capture device of claim 1, wherein the user authentication credential sent by the single mobile client application is used to authenticate a user on the user data publishing website and publish the new-data for private use on the user data publishing website.

The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [3]. *See, supra*, [7.11]. For example, Kahn teaches uploading images to an image server. See, e.g., TTI-1017, [0056], [0058]. Kahn teaches that images can be "published" in an album for the user. *Id*., [0012], [0065], [0074], [0077], [0089], FIG. 6

Claim 9

[9.P] A short-range wireless enabled data capture device, comprising:

972. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious

[9.P]. In my opinion, Hiroishi-Kahn-Endsley-Bluetooth teaches a short-range wireless enabled data capture device. Supra [1.P].

[9.1] a memory device;

973. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [9.1]. In my opinion, Hiroishi-Kahn-Endsley-Bluetooth teaches a memory device. Supra [1.1].

[9.2] a processor coupled to the memory device;

974. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [9.2]. In my opinion, Hiroishi-Kahn-Endsley-Bluetooth teaches a processor coupled to the memory device. Supra [1.2].

[9.3.1]-[9.3.2] a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone,
wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled data capture device cryptographically authenticating identity of the short-range wireless enabled cellular phone;

975. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [9.3.1]-[9.3.2]. In my opinion, Hiroishi-Kahn-Endsley-Bluetooth teaches a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone, wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled data capture device cryptographically authenticating identity of the short-range wireless

enabled cellular phone. Supra [1.3.1]-[1.3.2].

[9.4] a data capture circuitry;

976. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [9.4]. In my opinion, Hiroishi-Kahn-Endsley-Bluetooth teaches a data capture circuitry. Supra [1.4].

[9.5.1]-[9.5.2] said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;

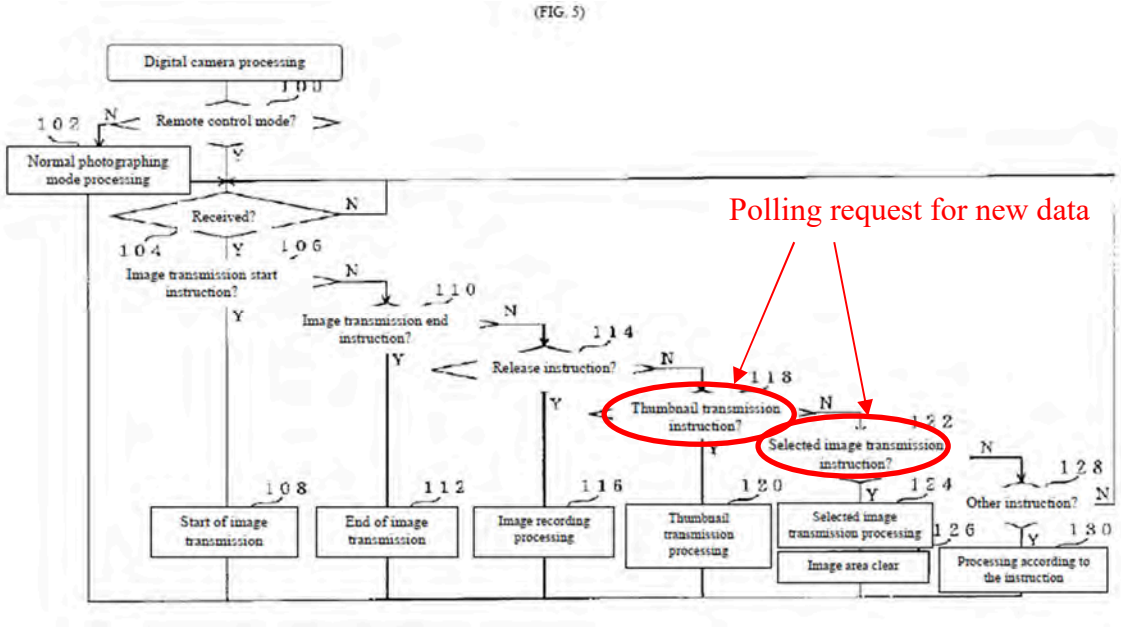
977. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [9.5.1]-[9.5.2]. In my opinion, Hiroishi-Kahn-Endsley-Bluetooth teaches said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone. Supra [1.5.1]-[1.5.2].

[9.6] said processor further configured to store the new-data in the memory device of the short-range wireless enabled data capture device;

978. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [9.6]. In my opinion, Hiroishi-Kahn-Endsley-Bluetooth teaches said processor further configured to store the new-data in the memory device of the short-range wireless enabled data capture device. Supra [1.6].

[9.7.1] said processor further configured to listen to a polling request from a single mobile client application on the short-range wireless enabled cellular phone, over the established paired short-range wireless connection, wherein the polling request is for the new-data,

979. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [9.7.1]. Hiroishi teaches that the processor is configured to listen to a polling request from the single mobile client application on the mobile phone. Specifically, Hiroishi teaches that the camera is controlled by operations sent by the mobile phone. *See, e.g.*, Hiroishi, [0068] (listing instructions sent to camera for mobile phone during remote mode of operation). As shown in FIG. 5, the camera listens for the reception of an instruction (polling request) from the mobile phone, including an instruction for the new data (the image stored in memory). FIG. 5 is reproduced below:



Hiroishi, FIG. 5 (annotated).

980. In one example, Hiroishi's thumbnail transmission instruction shown in flowchart symbol 118 is a polling request for the new data (images stored in camera memory). Note that in FIG. 5, the camera is checking (polling) for instructions from the mobile phone at flowchart symbol 104, and after the instruction is received checks which instruction at 106, 110, 114, 122, and 128 where 118 question answer, if "Yes", is the Thumbnail transmission instruction that requests the camera to send an indication of the new data captured by the camera and stored in memory. *See, e.g.*, Hiroishi, [0081]-[0082], [0104]-[0105]. In response, the camera sends the thumbnails to the mobile phone, which detects the new data (images) stored in memory through the thumbnails provided to the

client application and presented to the user on the GUI. *Id*. The thumbnails give the user and the client application an indication (or detection) of the images stored in memory (the new data).

981. In another example, the selected images for transmission instruction constitutes the polling request. *See, e.g.*, Hiroishi, [0084], [0104]-[0106]. When the mobile phone sends the selected images for transmission instruction, the camera automatically processes the selected images and automatically transmits the images to the mobile phone across the Bluetooth connection. *See, e.g.*, *id*.

982. Note that in Hiroishi, the program running on the mobile phone operates to send the polling request message, as required by the claim. The Patent Owner appears to assert that operations of polling "inherent" to Bluetooth satisfy this claim limitation. Note that Bluetooth operations like polling are not carried out by the client application (or any other application layer entity). Instead, such Bluetooth operations are carried out by the operating system or other lower layer function. To the extent that the Patent Owner's assertions are adopted, I note that Hiroishi teaches Bluetooth. One aspect taught by Bluetooth is polling. *See, e.g.*, Bluetooth Core Specification V2.1, 332 (8.6.1 Polling in active mode). In so far as the patent owner argues that polling is inherent to Bluetooth, Hiroshi's reliance on Bluetooth would likewise satisfy this claim limitation. For that reason, in addition to others described above, Hiroishi renders this element invalid.

[9.7.2]-[9.8] wherein the single mobile client application on the short-range wireless enabled cellular phone is configured to detect the new-data for transfer from the short-range wireless enabled data capture device to the paired and the cryptographically authenticated short-range wireless enabled cellular phone, wherein detecting the new-data for transfer comprises: polling the short-range wireless enabled data capture device by the short-range wireless enabled cellular phone, using the single mobile client application on the short-range wireless enabled cellular phone, over the established paired short-range wireless connection

983. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [9.7.2]-[9.8]. See supra, [9.7.1]. Hiroishi-Kahn-Endsley-Bluetooth teaches that the single mobile client application is configured to detect the new data for transfer polling the short-range wireless enabled data capture device by the short-range wireless enabled cellular phone, using the single mobile client application on the short-range wireless enabled cellular phone, over the established paired short-range wireless connection. Hiroishi detects the new data by sending a thumbnail transmission instruction to the camera and by receiving thumbnails from the camera in response. *See, e.g.*, Hiroishi, [0102]-[0105], FIGS. 5, 6, 7C.

984. Likewise, the selected image transmission instruction constitutes a polling request sent for the program running on the mobile phone to the camera. The selected image transmission instruction is a request for images to be transferred to the mobile phone for subsequent transmission to the remote terminal. *See, e.g.*, Hiroishi, [0084], [0106].

985. As I mentioned above, in Hiroishi, the program running on the mobile

phone operates to send the polling request message, as required by the claim. The Patent Owner appears to assert that operations of polling "inherent" to Bluetooth satisfy this claim limitation. Bluetooth operations like polling are not carried out by the client application (or any other application layer entity). Instead, such Bluetooth operations are carried out by the operating system or other lower layer function. To the extent that the Patent Owner's assertions are adopted, I note that Hiroishi teaches Bluetooth. One aspect taught by Bluetooth is polling. *See, e.g.*, Bluetooth Core Specification V2.1, 332 (8.6.1 Polling in active mode). In so far as the patent owner argues that polling is inherent to Bluetooth, Hiroshi's reliance on Bluetooth would likewise satisfy this claim limitation. For that reason, in addition to others described above, Hiroishi renders this element invalid.

[9.9]-[9.16] said processor further configured to transfer the new-data from the short-range wireless enabled data capture device to the short-range wireless enabled cellular phone automatically over the established paired short-range wireless connection,
wherein the single mobile client application on the short-range wireless enabled cellular phone is further configured to receive the new-data over the established short-range paired wireless connection,
wherein the single mobile client application on the short-range wireless enabled cellular phone is further configured to store the received new-data in a memory device of the short-range wireless enabled cellular phone,
wherein the single mobile client application for the short-range wireless enabled cellular phone stores a user authentication credential in the memory device of the short-range wireless enabled cellular phone,
wherein the single mobile client application on the short-range wireless enabled cellular phone is further configured to use HTTP to send a user preference to a user data publishing website over a cellular data network,
wherein the user preference comprise global positioning system information,
wherein the single mobile client application on the short-range wireless

enabled cellular phone is further configured to use the HTTP to upload the received new-data and the user authentication credential to the user data publishing website over the cellular data network,
wherein the upload is based on a timer setting on the single mobile client application, and
wherein the timer setting is no wait automatic or wait X minutes automatic, and
wherein the single mobile client application on the short-range wireless enabled cellular phone provides a touch based GUI for the received new-data.

986. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [9.9]-[9.16]. See supra, [7.10]-[7.12].

987. In the combination, Hiroishi teaches that the camera's processor transmits the images to the mobile phone automatically after the polling request message is received. Note that in the 121 specification, it states that the transfer of images occurs automatically after polling. *See, e.g.*, '121 patent, 4:60-67. In Hiroishi, the camera transfers the images (the new data) from the camera to the phone "automatically" after the camera receives the polling request (the selected images for transfer request). Part of the automation in Hiroishi is that the camera has to process the images for transfer without further instruction or input from the user. Specifically, Hiroishi teaches that "a selected image transmission processing is performed," on the images to be transmitted. Hiroishi, [0084]. The "selected image transmission processing is that the digital image data corresponding to the image selected by the operator of the mobile phone 40 from a plurality of images shown by the thumbnails transmitted according to the thumbnail transmission

instruction information is read from the photographed image data storage area of SDRAM 55A (not shown) is transmitted to the mobile phone 40." *Id*. Though not explicitly stated, it is inherent in Hiroishi that the image data is packetized for transmission across the Bluetooth channel using standard Bluetooth packet encoding, as taught by Bluetooth Core Specification V2.1, 272 et. seq. This packetization also constitutes part of the automation involved in Hiroishi the camera uses to transmit the images across the Bluetooth connection to the mobile phone.

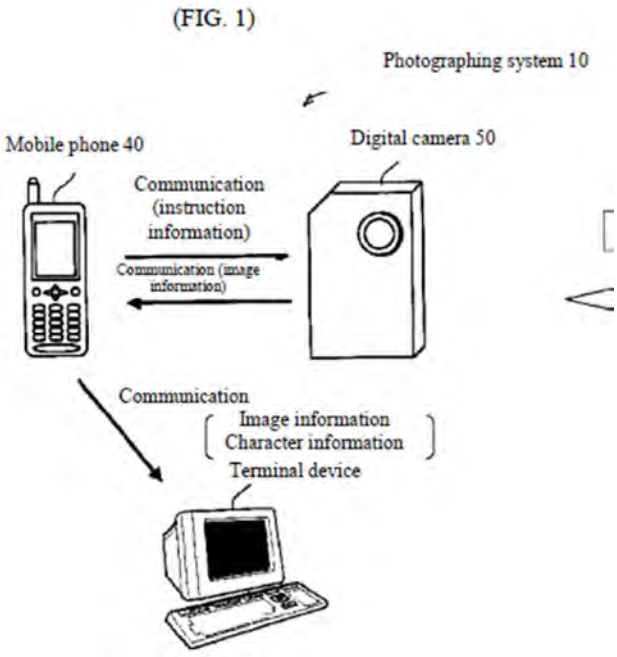
[10] The short-range wireless enabled data capture device of claim 9, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

988. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [10]. Supra [2], [8].

Claim 4

[4.P] A system, comprising:

989. To the extent the preamble is limiting, the Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.P]. Hiroishi teaches a system that includes a mobile phone in control of a camera by a Bluetooth connection; the system of Hiroishi can also include that the mobile phone is in communication with a remote terminal across the Internet by way of a cellular data network. *See, e.g.*, Hiroishi, FIGS. 1-2:



Hiroishi, FIG. 1 (annotated)

Hiroishi describes FIG. 1 as showing a "photographing system 10." *Id*. The photographing system 10 includes a digital camera 50, a mobile phone, and the terminal device. *Id*.

[4.1] a short-range wireless enabled data capture device, comprising:

990. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.1]. Supra [1.P].

[4.2] a first memory device;

991. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.2]. Supra [1.1].

[4.3] a first processor coupled to the first memory device;

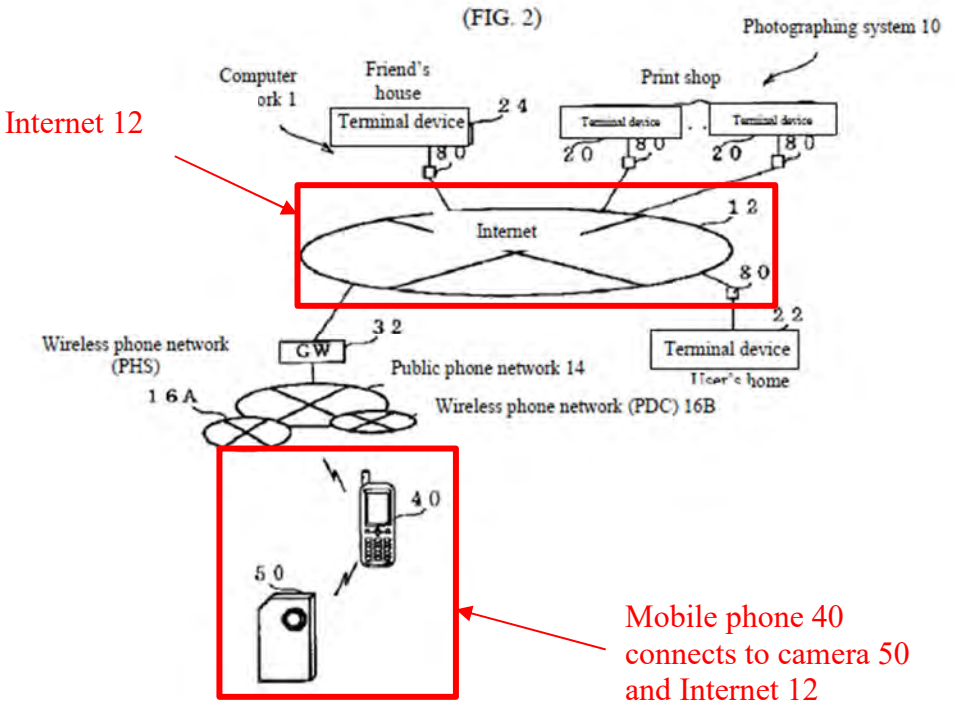
992. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious

[4.3]. Supra [1.2].

[4.4.1]-[4.4.3] a first short-range wireless communication device configured to establish a short-range paired wireless connection with a short-range wireless enabled cellular phone, wherein the short-range wireless enabled cellular phone is internet enabled, wherein establishing the short-range paired wireless connection comprises, the short-range wireless enabled data capture device cryptographically authenticating identity of the short-range wireless enabled cellular phone;

993. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.4.1]-[4.4.3]. Supra [1.3.1]-[1.3.2]. In the combination, Hiroishi teaches that the mobile phone 40 is Internet enabled. *See, e.g.*, Hiroishi, [0047]-[0049], [0122], FIG. 2.

994. Hiroishi-Kahn-Endsley-Bluetooth renders obvious [4.4.2]. In the combination, the cellular phone (Hiroishi's mobile phone 40) is internet enabled. *Id*.; Hiroishi, [0052] (confirming that Hiroishi's phone 40 includes a "communication control unit 44" that is "connected to a transceiver 45 for modulating … packet information"). Hiroishi's phone 40 includes a web browser. *Id*., [0122]. And, as shown in FIG. 2, Hiroishi's "computer network 1 comprises the Internet 12." Hiroishi, [0047].



TTI-1011, FIG. 2 (annotated).

[4.5] a data capture circuitry;

995. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.5]. Supra [1.4].

[4.6.1]-[4.6.2] said first processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection with the short-range wireless enabled cellular phone;

996. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.6]. Supra [1.5.1]-[1.5.2].

[4.7] said first processor further configured to store the new-data in the first memory device; and

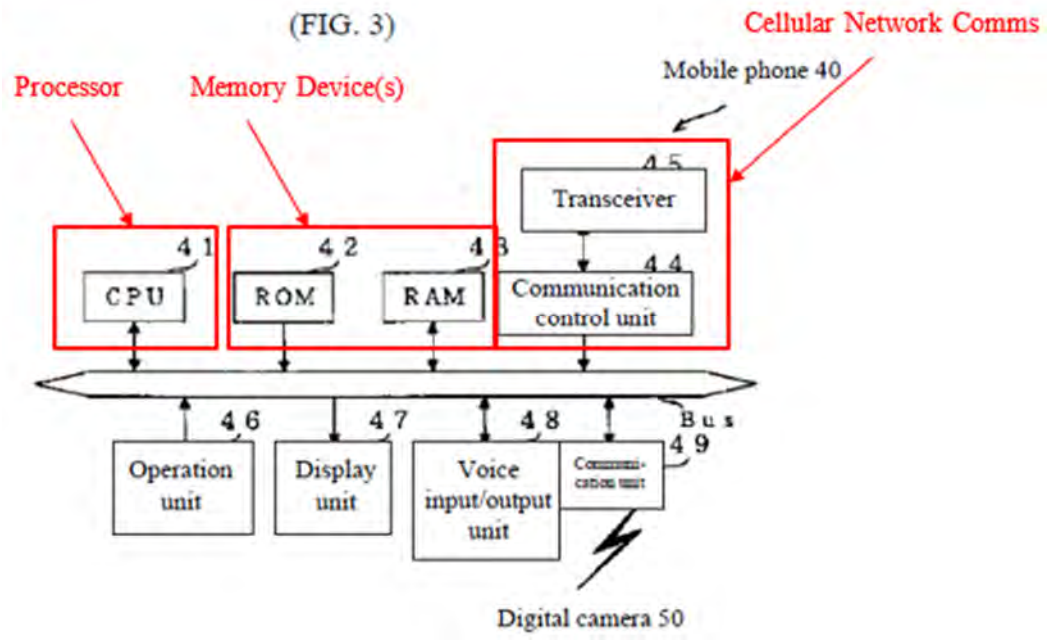
997. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.7]. Supra [1.6].

[4.8.1]-[4.8.2] said first processor further configured to send an event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically,
wherein the event notification corresponds to the acquired new-data and comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone;

998. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.8.1]-[4.8.2]. Supra [1.7.1]-[1.7.2].

[4.9] said short-range wireless enabled cellular phone, comprising: a second memory device;

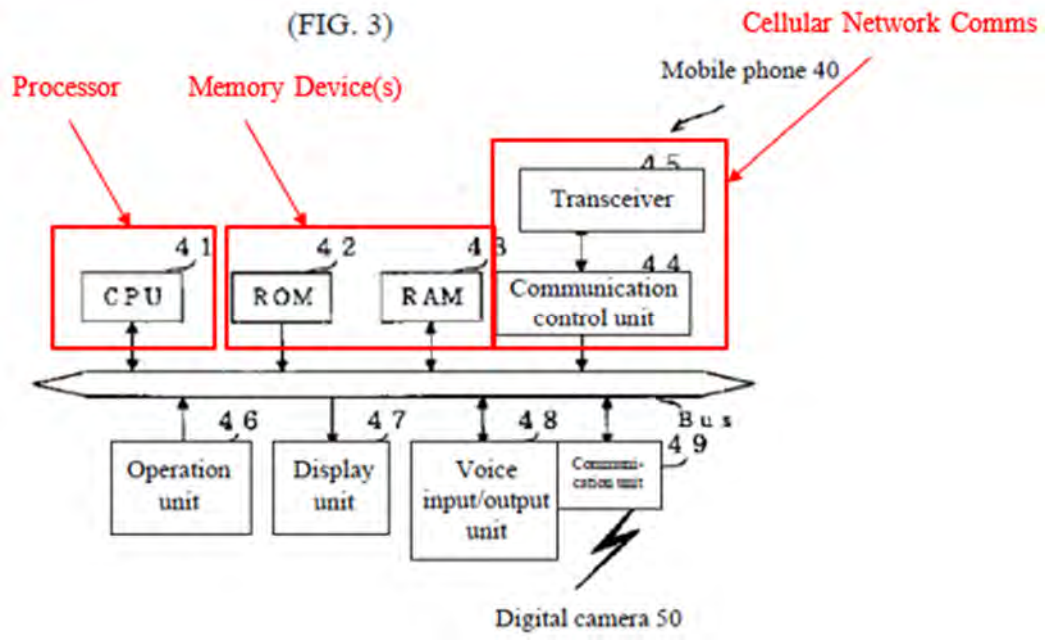
999. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.9]. Supra [7.P]. In the combination, Hiroishi's phone 40 includes a memory device (RAM 43) and a processor (CPU 41) coupled to the memory device. TTI-1011, [0051], FIG. 3.



TTI-1011, FIG. 3.

[4.10] a second processor coupled to the second memory device;

1000. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.10]. Supra [7.1]. In the combination, Hiroishi's phone 40 includes a memory device (RAM 43) and a processor (CPU 41) coupled to the memory device. TTI-1011, [0051], FIG. 3.



TTI-1011, FIG. 3.

[4.11] a cellular network communication device configured to connect to the internet via a cellular data network;

1001. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.11]. Hiroishi-Kahn-Endsley-Bluetooth teaches a cellular network communication device configured to connect to the internet via a cellular data network. Supra [7.3].

[4.12] a second short-range wireless communication device configured to establish the short-range paired wireless connection between the short-range wireless enabled cellular phone and the short-range wireless enabled data capture device;

1002. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.12]. Hiroishi-Kahn-Endsley-Bluetooth teaches a second short-range wireless communication device configured to establish the short-range paired wireless

connection between the short-range wireless enabled cellular phone and the short-range wireless enabled data capture device. Supra [7.4].

[4.13] a single mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that, when executed by the second processor controls the second processor to:

1003. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.13]. Hiroishi-Kahn-Endsley-Bluetooth teaches a single mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that are executed by the second processor. Supra [7.5].

[4.14] listen for the event notification sent by the short-range wireless enabled data capture device, wherein the single mobile client application for the short-range wireless enabled cellular phone is configured to process the event notification;

1004. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.15]. Hiroishi-Kahn-Endsley-Bluetooth teaches listen for the event notification sent by the short-range wireless enabled data capture device, wherein the single mobile client application for the short-range wireless enabled cellular phone is configured to process the event notification. Supra [7.6]. [1.8]-[1.9]

[4.15] receive the new-data from the short-range wireless enabled data capture device;

1005. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.15]. Hiroishi-Kahn-Endsley-Bluetooth teaches receive the new-data from the short-range wireless enabled data capture device. Supra [7.7].

[4.16] store the received new-data in the second memory device;

1006. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.16]. Hiroishi-Kahn-Endsley-Bluetooth teaches store the received new-data in the second memory device. Supra [7.8].

[4.17] store a user authentication credential in the second memory device;

1007. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.17]. Hiroishi-Kahn-Endsley-Bluetooth teaches store a user authentication credential in the second memory device. Supra [1.9].

[4.18] use HTTP to upload the received new-data and the user authentication credential to a user data publishing website over the cellular data network, wherein the upload is based on a timer setting on the single mobile client application, and wherein the timer setting is no wait automatic or wait X minutes automatic;

1008. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.18]. Hiroishi-Kahn-Endsley-Bluetooth teaches using HTTP to upload the received new-data and the user authentication credential to a user data publishing website over the cellular data network, wherein the upload is based on a timer setting on the single mobile client application, and wherein the timer setting is no wait automatic or wait X minutes automatic. Supra [7.10] and [7.11].

[4.19] 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

1009. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.19]. Hiroishi-Kahn-Endsley-Bluetooth teaches using 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. Supra [7.10].

[4.20] provide a touch based graphical user interface for the received new-data.

1010. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [4.20]. Hiroishi-Kahn-Endsley-Bluetooth teaches provide a touch based graphical user interface for the received new-data. Supra [7.12].

[5] The system of claim 4, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

1011. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [5]. Hiroishi-Kahn-Endsley-Bluetooth teaches the short-range paired wireless connection is a Bluetooth paired wireless connection. Supra [8].

[6] The system of claim 4, wherein the user authentication credential is for a user of the user data publishing website.

1012. The Hiroishi-Kahn-Endsley-Bluetooth combination renders obvious [6]. Hiroishi-Kahn-Endsley-Bluetooth teaches the user authentication credential is for a user of the user data publishing website. Supra [3].

B. Ground 2: Singh129 renders claims 1-10 obvious

1013. Singh129 provides the same disclosure as the ’121 patent, including the subject matter disclosed in Singh906 that is incorporated by reference. *Compare* ’121 patent *with* Singh129. Singh906 provides the same disclosure as

the incorporated ’802 application. It would have been obvious to combine Singh129 with teachings found in Singh906 to arrive at the Challenged Claims. The disclosure demonstrates that it would have been obvious in view of Singh906 to modify Singh129’s user preferences to include authentication credentials and global positioning system information and modify Singh129’s client application 203 to include a user authentication module that can log on to websites on the user’s behalf and publish the content.

1014. A person of ordinary skill in the art would have been motivated to make these modifications for several reasons. Indeed, adding authentication credentials and global position system information to Singh129’s user preferences would have given the user more control over the publishing of their multimedia content. Moreover, there was a known problem of associating multimedia objects with user preferences in the art as shown in Singh129. Singh906’s user preferences address that issue. And combining the teachings of Singh129 and Singh906 was not beyond the skill of ordinary skill in the art. Indeed, Singh129 and Singh906 address the same problem of associating multimedia objects with user preferences. Thus, Singh906’s user preferences, which included authentication credentials and global positioning information, were a known way to address that problem.

1015. A person of ordinary skill in the art would have been further

motivated to modify Singh129's client application to upload user preferences (e.g., authentication credentials and GPS information) to websites so that the client application can publish content on websites that require such information without first sending those preferences to a publishing service. A person of ordinary skill in the art would have understood that this functionality would increase the speed at which content could be uploaded because it would reduce the number of data transmissions. For mobile devices with sufficient memory to store the content received from the data capture device, it also would have reduced the need to host a separate publishing service and therefore reduced complexity and cost. And even if the publishing service was included in the combination, the mobile device would still be able to publish content when the publishing service was down (*e.g.*, for maintenance or due to a power outage).

1016. A POSITA would have had a reasonable expectation of success when combining Singh129's disclosures as described above. Indeed, the proposed combination would have required no more than the application of known techniques (using authentication credentials and GPS information) to a known system (Singh129's system) in the same field of endeavor (media publishing) and from the same assignee (CellSpinSoft) to obtain the benefits described above. Furthermore, in the combination, each element performs the same predictable function as it does separately, without significantly hindering the functions

performed by Singh129's system. Indeed, Singh129's system would have continued to perform all the functions it performed before the proposed modifications, including associating multimedia content with user preferences.

1017. The Singh129 combination renders obvious each element of claims 1-10 of the '121 patent.

[1.P]. A short-range wireless enabled data capture device, comprising:

1018. To the extent the preamble is limiting, the Singh129 combination renders obvious element [1.P]. For example, the Singh129 combination includes digital data capture device 201 (*e.g.*, a camera), which includes Bluetooth communication device 201a that enables short-range wireless communication with Bluetooth enabled mobile device 202. TTI-1009, Figs. 2, 5.

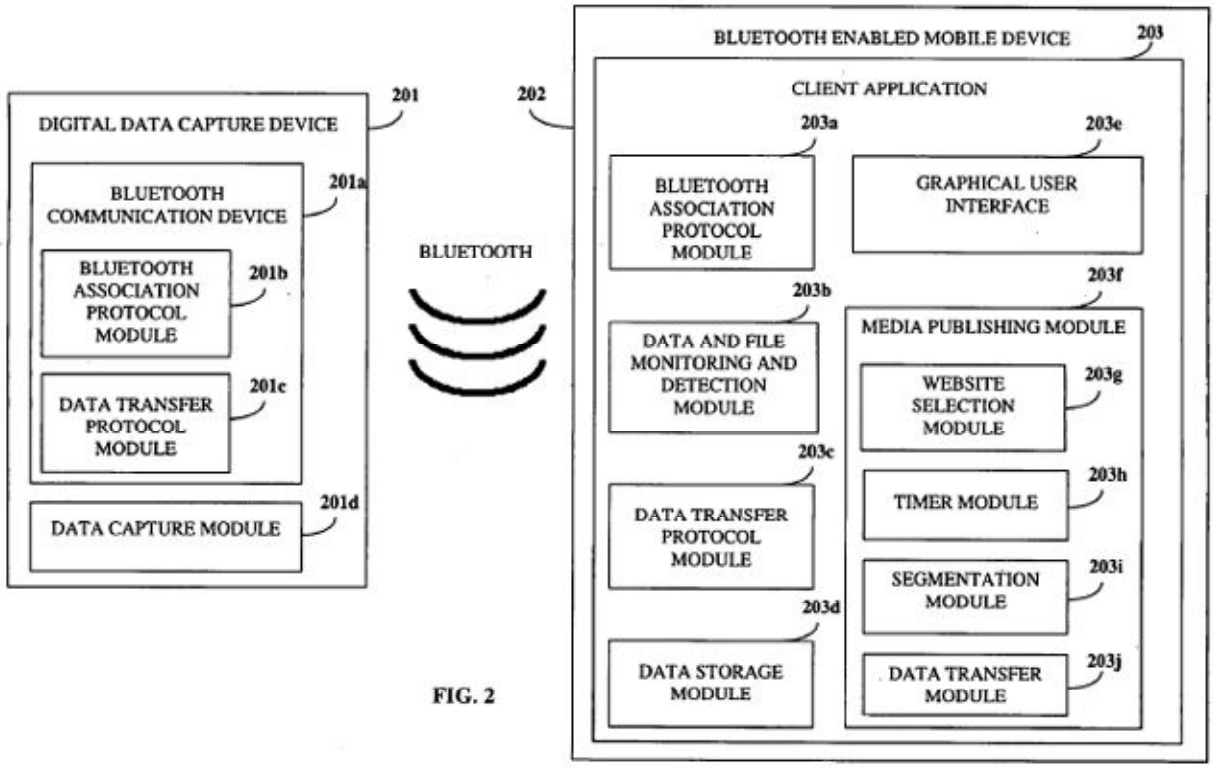


FIG. 2

TTI-1009, Fig. 2.

[1.1] a memory device;

1019. The Singh129 combination renders obvious element [1.1]. The Singh129 combination's data capture device includes a memory devices, "one or more microprocessors will receive instructions from a memory or like device", TTI-1009, [0048] and the memory portion of BT memory card 302). TTI-1009, [0008], [0020], [0032], [0041], Figs. 2, 3A.

[1.2] a processor coupled to the memory device;

1020. The Singh129 combination renders obvious element [1.2]. The Singh129 combination's data capture device includes a processor coupled to the memory device. TTI-1009, [0048], ("It will be readily apparent that the various methods and algorithms described herein may be implemented in a computer readable medium appropriately programmed for general purpose computers and computing devices. Typically, a processor, for e.g., one or more microprocessors will receive instructions from a memory or like device, and execute those instructions."').

[1.3.1] a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone,

1021. The Singh129 combination renders obvious element [1.3]. The

Singh129 combination includes a short-range wireless communication device (Bluetooth communication device 201a) configured to establish (via the Bluetooth protocol) a short-range paired wireless connection between the short-range wireless enabled data capture device 201 and a short-range wireless enabled cellular phone (Bluetooth enabled mobile device 202, which can be a cellular phone). TTI-1009, [0021]-[0022], [0046], Figs. 1-2.

[1.3.2] wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled data capture device cryptographically authenticating identity of the short-range wireless enabled cellular phone;

1022. The Singh129 combination renders obvious element 1.3.2. In the Singh129 combination, establishing the short-range paired wireless connection comprises the data capture device cryptographically authenticating (via the Bluetooth protocol; specifically exchanging passkeys) the identity the cellular phone. TTI-1009, [0021]-[0022] ("A BT device that wants to communicate only with a trusted device can cryptographically authenticate the identity of another BT device.").

[1.4] a data capture circuitry;

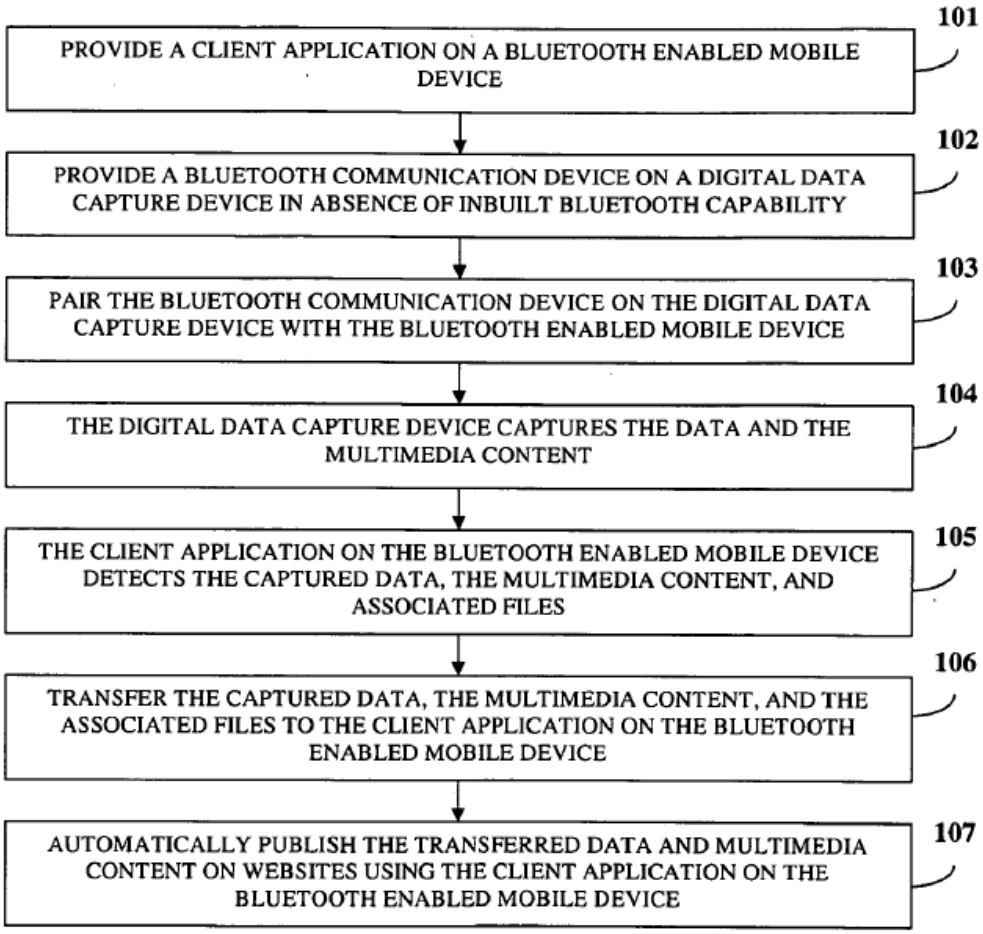
1023. The Singh129 combination renders obvious element 1.4. The Singh129 combination includes a data capture circuity (data capture module 201d). TTI-1009, [0031], Fig. 2.

[1.5.1] said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry,

1024. The Singh129 combination renders obvious element [1.5.1]. The Singh129 combination's processor (*see* element [1.2]) is configured to acquire new-data (e.g., images) in the data capture device 201 using the data capture circuitry 201d. TTI-1009, [0033] ("The data capture module 201d captures the data and the multimedia content on the digital data capture device 201."), [0023], [0041], [0048], Figs. 1, 2, 5.

[1.5.2] wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;

1025. The Singh129 combination renders obvious element [1.5.2]. As shown in Figure 1 of Singh129, the new-data is data acquired (in step 104) after establishing the short-range wireless connection (in step 103) between the data capture device 201 and the cellular phone (mobile device 202). TTI-1009, Fig. 1, [0021]-[0023].



TTI-1009, Fig. 1.

[1.6] said processor further configured to store the new-data in the memory device;

1026. The Singh129 combination renders obvious element [1.6]. The Singh129 combination's processor (*see* element [1.2]) is further configured to store the new-data in the memory device (*see* element [1.1]). TTI-1009, [0023], Figs. 1, 5. As explained in Singh129, the "user captures 104 data and multimedia content using the digital data capture device 201." TTI-1009, [0023]; *see also* [0041] ("the user 502 may capture an image using the digital camera."). Accordingly, a person

of ordinary skill in the art would have understood that the processor stores the data and multimedia in the memory device.

[1.7.1] said processor further configured to send an event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically,

1027. The Singh129 combination renders obvious element [1.7.1]]. The Singh129's processor (*see* element [1.2]) is further configured to send an event notification ("a signal to the client application") and the acquired new-data to the cellular phone (mobile device 202) over the established short-range paired wireless (Bluetooth) connection automatically. TTI-1009, [0025] ("In the push mode, the BT communication device 201a sends a signal to the client application 203 on creation of a new file. By implementation of a handshake protocol, the BT communication device 201a automatically transfers captured data, the multimedia content, and the associated files to the client application on the mobile device 202.").

[1.7.2] wherein the event notification corresponds to the acquired new-data and comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone,

1028. The Singh129 combination renders obvious element [1.7.2]. In the Singh129 combination, the event notification corresponds to the acquired new-data (because it is sent when the new-data is acquired and informs the cellular phone that the new-data is available) and comprises sending a signal (a response to a poll

from client application 203 or a signal sent to client application 203 on creation of a new file) to the cellular phone. TTI-1009, [0023] ("In the pull mode, the client application 203 periodically polls the digital data capture device 201 to determine the creation of a new file in the digital data capture device 201. 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."), [0025] ("In the push mode, the BT communication device 201a sends a signal to the client application 203 on creation of a new file. By implementation of a handshake protocol, the BT communication device 201a automatically transfers captured data, the multimedia content, and the associated files to the client application on the mobile device 202.").

[1.8] wherein the cryptographically authenticated short-range wireless enabled cellular phone is configured to listen to the event notification and receive the new-data over the established short-range paired wireless connection,

1029. The Singh129 combination renders obvious element [1.8]. In the Singh129 combination, the cellular phone is configured to listen (via data and file monitoring and detection module 203b) to the event notification signal and receive (via data transfer protocol module 203c) the new-data over the established short-range paired wireless (Bluetooth) connection. TTI-1009, Fig. 2, [0033]-[0034] ("The data and file monitoring and detection module 203b of the client application

203 monitors and detects the capture of the data, the multimedia content, and the files associated with the captured data and the multimedia content. On detection, the data transfer protocol module 203c of the client application 203 initiates the transfer and download of the captured data, the multimedia content, and the associated files from the digital data capture device 201."), [0023]-[0025] (describing the push and pull modes).

[1.9.1]-[1.9.2] wherein a single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the event notification and store the received new-data in a memory device of the cryptographically authenticated short-range wireless enabled cellular phone,

1030. The Singh129 combination renders obvious element [1.9.1]-[1.9.2]. In the Singh129 combination a single mobile client application (Singh129's client application 203 modified to include user preferences comprising user authentication and GPS information as taught by Singh906) for the cellular phone is configured to process the event notification (using data and file monitoring and detection module 203b and/or Bluetooth association protocol module 203a) and store the received new-data in a memory device (data storage module 203d) of the cellular phone. TTI-1009, [0033]-[0035] ("The data and file monitoring and detection module 203b of the client application 203 monitors and detects the capture of the data, the multimedia content, and the files associated with the captured data and the multimedia content. … The data storage module 203d stores

the captured data, the multimedia content, and the associated files on the mobile device 202."), [0023]-[0025] (describing the push and pull modes), Fig. 2.

[1.10] wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone stores a user authentication credential in the memory device of the cryptographically authenticated short-range wireless enabled cellular phone,

1031. The Singh129 combination renders obvious element [1.10]. In the Singh129 combination, the single mobile client application (*see* element [1.9]) for the cellular phone stores a user authentication credential (*e.g.*, "authentication ID" or "authentication credentials" as taught by Singh906) and the memory device (*see* element [1.9]) of the cellular phone. TTI-1010, Fig. 2 (showing user authentication module 202e), Fig. 4 ("authentication ID"), [0023] ("The user preferences may comprise authentication credentials…."), [0025]-[0026] ("user authentication module 202e), [0028] ("The preferences set by the user 201 may be authentication credentials…."); TTI-1009, Figs. 2, 4 (showing client application 203), [0033]-[0037] (describing same).

[1.11] wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to use HTTP to upload the received new-data and the user authentication credential to a user data publishing website over a cellular data network,

1032. The Singh129 combination renders obvious element [1.11]. In the Singh129 combination, the single mobile client application (*see* element [1.9]) is configured to use HTTP to upload the received new-data and the user

authentication credential to a user data publishing website ("for example, Flickr™, Picasa™, YouTube™, eBay®, etc.") over a cellular data network (Singh129's "cellular network"). TTI-1009, Fig. 1, [0029], [0045] [0047]. As explained in Singh129, "client application 203 on the mobile device 202 … automatically publishes 107 the transferred data and multimedia content on one or more websites." TTI-1009, [0029], Fig. 1; *see also* [0045] (similar). And, as explained in Singh906, "[t]he multimedia object is transferred with the user authentication credentials to the [website]" by a publishing service. TTI-2005, [0037]; *see also* [0047] (similar). In the combination, however, the media is transferred with the user authentication credentials to the website by the client application.

1033. As further explained in Singh129, "[t]he network 402 may, for example, be a … cellular network…." TTI-1009, [0039]. And "[t]he transport protocol that is used between the client application 203 and the publishing service 401 may be hypertext transfer protocol (HTTP)…." TTI-1009, [0047]. In the Singh129 combination, HTTP is also used between the client application and the website. *See* Ground 2, [1.9.1]-[1.9.2].

[1.12] wherein the upload is based on a timer setting on the single mobile client application, wherein the timer setting is no wait automatic or wait X minutes automatic,

1034. The Singh129 combination renders obvious element [1.12]. In the Singh129 combination, the upload is based on a timer setting (the "no-wait-

automatic," "wait-X-minutes-automatic," or "wait-X-minutes-user-input-cancel" settings in Singh129's timer module 203h, which "sets the time for publishing") on the single mobile client application.; TTI-1009, [0036].

[1.13] 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

1035. *See* Ground 2, Element [1.11] (confirming that the Singh129 combination's single mobile client application is configured to use HTTP to send the user authentication credential to the user data publishing website over the cellular data network). As confirmed in Singh129, the user authentication credential is a user preference. TTI-1010, [0023] ("The user preferences may comprise authentication credentials….").

[1.14] 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.

1036. The Singh129 combination renders obvious element [1.14]. In the Singh129 combination, the single mobile client application for the cellular phone provides a touch-based GUI ("graphical user interface 202a") for the received new-data. *Id*.; TTI-1009, Fig. 2, [0033] ("graphical user interface (GUI) 203e"), [0035] ("The user may also set preferences on the mobile device 202 using the GUI 203e of the client application203."), Claim 11 (similar).

[2] The short-range wireless enabled data capture device of claim 1, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

1037. The Singh129 combination renders obvious claim 2. In the Singh129 combination, the short-range paired wireless connection is a Bluetooth paired wireless connection. *Id*.; TTI-1009, Fig. 1, [0021].

[3] The short-range wireless enabled data capture device of claim 1, wherein the user authentication credential sent by the single mobile client application is used to authenticate a user on the user data publishing website and publish the new-data for private use on the user data publishing website.

1038. The Singh129 combination renders obvious claim 3. In the Singh129 combination, the user authentication credential (*e.g*., "authentication ID" or "authentication credentials" as taught by Singh906) sent by the single mobile client application is used to authenticate (using Singh906's user authentication module 204g, which is incorporated into Singh129's publishing service 401) a user on the user data publishing website and publish the new-data for private use on the user data publishing website. TTI-1009, Fig. 1 (step 107), [0029]; TTI-1010, Fig. 4 (steps 410-411), [0035] ("The user authentication module 204g authenticates the user 201 of the client application…."), [0037] ("The user 201 is authenticated [using the authentication credentials] before publishing the user created multimedia content on the chosen publication virtual spaces 205."), [0049] ("The front end service 204b associates the multimedia object with the user preferences stored in

the database 204a, authenticates 410 the user 201 for a particular publication virtual space and then publishes 411 the multimedia object on the selected publication virtual spaces 205.").

[4.P] A system, comprising:

1039. To the extent the preamble is limiting, the Singh129 combination renders obvious element [1.P]. The Singh129 combination includes a system comprising, among other things, a digital data capture device 201, a Bluetooth enabled mobile device 202, and a publishing service 401. TTI-1009, Figs. 1-5 and related descriptions.

[4.1]-[4.4.1]

1040. *See* Ground 2, Elements [1.P]-[1.3.1].

[4.4.2] wherein the short-range wireless enabled cellular phone is internet enabled,

1041. The Singh129 combination renders obvious element [4.4.2]. In the Singh129 combination, the cellular phone is internet enabled. TTI-1009, [0039], [0042] ("The client application 203 automatically publishes the transferred image on one or more websites via the internet 501."), [0047 ("One of the transport mechanisms to achieve the connectivity between the publishing service 401 and the client application 203 is the wireless internet. ... 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.").

[4.4.3]-[4.8.2]

1042. *See* Ground 2, Elements [1.3.2]-[1.7.2].

[4.9] said short-range wireless enabled cellular phone, comprising: a second memory device;

1043. The Singh129 combination renders obvious element [4.9]. The Singh129 combination's cellular phone comprises a memory device (data storage module 203d). TTI-1009, Fig. 2, [0033], [0035] ("The data storage module 203d stores the captured data, the multimedia content, and the associated files on the mobile device 202.").

[4.10] a second processor coupled to the second memory device;

1044. The Singh129 combination renders obvious element [4.10]. The Singh129 combination's cellular phone comprises a processor coupled to the second memory device. TTI-1009, [0026] (disclosing a "mobile device 202 with limited memory and processing capabilities"), [0037] (similar), [0039] (similar), [0043] (similar), [0048] ("[T]he various methods and algorithms described [in Singh129] may be implemented in a computer readable medium appropriately programmed for general purpose computers and computing devices. Typically, a processor, for e.g., one or more microprocessors will receive instructions from a memory or like device, and execute those instructions, thereby performing one or more processes defined by those instructions.").

[4.11] a cellular network communication device configured to connect to the internet via a cellular data network;

1045. The Singh129 combination renders obvious element [4.11]. The Singh129 combination's cellular phone comprises a cellular network communication (the portion of the phone that enables telephony data capabilities and/or data transfer module 203j) configured to connected to the internet via a cellular data network ("telephony network" or "cellular network"). TTI-1009, [0039] ("The network 402 may, for example, be a … cellular network…."), [0047] ("the mobile phones may transfer data to the publishing service 401 over the telephony network at near broadband speeds … mobile phones equipped with both wireless network and telephony data capabilities may use either of the two to communicate with the publishing service 401").

[4.12] a second short-range wireless communication device configured to establish the short-range paired wireless connection between the short-range wireless enabled cellular phone and the short-range wireless enabled data capture device;

1046. The Singh129 combination renders obvious element [4.12]. The Singh129 combination's cellular phone comprises a second short-range wireless communication device (Bluetooth association protocol module 203a) configured to establish the short-range paired wireless (Bluetooth) connection between the cellular phone and the data capture device. TTI-1009, Fig. 2, [0033] ("The BT association protocol module 201b of the digital data capture device 201 and the BT association protocol module 203a of the client application 203 enable the pairing between the BT communication device 201a and the mobile device 202.").

[4.13]-[4.14.1] a single mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that, when executed by the second processor controls the second processor to: listen for the event notification sent by the short-range wireless enabled data capture device,

1047. The Singh129 combination renders obvious element [4.13]-[4.14.1]. The Singh129 combination's cellular phone comprises a single mobile client application (Singh129's client application 203 modified in accordance with Singh906) comprising executable instructions (BT association protocol module 201b and/or data and file monitoring and detection module 203b), that, when executed by the second processor, control the second processor to listen for the event notification sent by the data capture device. TTI-1009, Figs. 1-2, [0025] ("A file event listener in the client application 203 listens for the signal from the digital data capture device 201.").

[4.14.2] wherein the single mobile client application for the short-range wireless enabled cellular phone is configured to process the event notification;

1048. *See* Ground 2, Element [1.9].

[4.15] receive the new-data from the short-range wireless enabled data capture device;

1049. *See* Ground 2, Element [1.8].

[4.16]-[4.20]

1050. *See* Ground 2, Elements [1.9]-[1.14].

Claim 5

1051. *See* Ground 2, Claim 2.

Claim 6

1052. *See* Ground 2, Claim 3.

[7.P]

1053. *See* Ground 2, Element [1.3].

[7.1]-[7.4.1]

1054. *See* Ground 2, Elements [4.9]-[4.12].

[7.4.2]

1055. *See* Ground 2, Element [1.3.2].

[7.5]

1056. *See* Ground 2, Element [4.13].

[7.6.1]

1057. *See* Ground 2, Element [1.7.2]-[1.8].

[7.6.2]

1058. *See* Ground 2, Element [1.5.2].

[7.7] receive the event notification and the new-data from the short-range wireless enabled data capture device;

1059. *See* Ground 2, Element [1.8] (confirming that the Singh129 combination's client application is controls the processor to receive the new-data from the short-range wireless enabled data capture device). The Singh129 combination's client application also controls the processor to receive the event notification from the data capture device using BT association protocol module 201b and/or data and file monitoring and detection module 203b. TTI-1009,

[0023]-[0025], [0033].

[7.8]

1060. *See* Ground 2, Element [1.9].

[7.9]

1061. *See* Ground 2, Element [1.10].

[7.10]

1062. *See* Ground 2, Element [1.13].

[7.11]

1063. *See* Ground 2, Elements [1.11]-[1.12].

[7.12]

1064. *See* Ground 2, Element [1.14].

Claim 8

1065. *See* Ground 2, Claim 2.

[9.P]-[9.6]

1066. *See* Ground 2, Elements [1.P]-[1.6].

[9.7.1] said processor further configured to listen to a polling request from a single mobile client application on the short-range wireless enabled cellular phone, over the established paired short-range wireless connection, wherein the polling request is for the new-data,

1067. The Singh129 combination renders obvious element [9.7.1]. The processor in the Singh129 combination's data capture device 201 is configured to listen to a polling request from a single mobile client application (Singh129's client application 203 modified in accordance with Singh906) on the cellular phone

202, over the established paired Bluetooth connection, wherein the polling request is for the new-data. TTI-1009, [0023]-[0025] ("the client application 203 periodically polls the digital data capture device 201 to determine the creation of a new file in the digital data capture device 201.").

[9.7.2] wherein the single mobile client application on the short-range wireless enabled cellular phone is configured to detect the new-data for transfer from the short-range wireless enabled data capture device to the paired and the cryptographically authenticated short-range wireless enabled cellular phone,

1068. The Singh129 combination renders obvious element [9.7.2]. In the Singh129 combination, the single mobile client application on the cellular phone is configured to detect (using BT association protocol module 201b and/or data and file monitoring and detection module 203b) the new-data for transfer from the data capture device 201 to the cellular phone 202. TTI-1009, [0033], [0034] ("The data and file monitoring and detection module 203b of the client application 203 monitors and detects the capture of the data, the multimedia content, and the files associated with the captured data and the multimedia content.").

[9.8] wherein detecting the new-data for transfer comprises: polling the short-range wireless enabled data capture device by the short-range wireless enabled cellular phone, using the single mobile client application on the short-range wireless enabled cellular phone, over the established paired short-range wireless connection;

1069. The Singh129/Singh906 combination includes element [9.8]. TTI-1030, 1069. Singh129's single mobile client application 203 on cellular phone 202 is configured to detect (using Bluetooth association protocol module 201b and/or

data and file monitoring and detection module 203b) the new-data for transfer from the data capture device 201 to the cellular phone 202. TTI-1009, [0033], [0034]. The Singh129/Singh906 combination includes detecting the new-data for transfer by Singh129's cellular phone 202 comprises polling Singh129's data capture device 201 by the cellular phone 202 using the Singh129/Singh906 combination's client application over the established paired Bluetooth connection. TTI-1009, [0021]-[0022] (describing the paired connection), [0023] (describing polling), [0025] (describing the push mode)..

[9.9]-[9.10]

1070. *See* Ground 2, Element [1.8].

[9.11]

1071. *See* Ground 2, Element [1.9].

[9.12]]

1072. *See* Ground 2, Element [1.10].

[9.13]

1073. *See* Ground 2, Elements [1.13].

[9.14]-[9.15]

1074. See Ground 2, Elements [1.11]-[1.12].

[9.16]

1075. *See* Ground 2, Element [1.14].

Claim 10

1076. *See* Ground 2, Claim 2.

XIII. INVALIDITY ANALYSIS OF THE '381 PATENT

A. Ground 1: The Combination of Hiroishi, Kahn, and Bluetooth Render Claims 1-16 Obvious

1077. Hiroishi teaches a photographing system that includes a cellular phone that connects to a camera via a Bluetooth connection. *See, e.g.*, TTI-1011, [0042], [0066]-[0067]. The cellular phone can control the camera to capture images, store images, and transmit images to the cellular phone. *See, e.g.*, *id*., [0068]. The cellular phone can then transmit images to a remote computer destination by a cellular network connection via the Internet. *See, e.g.*, *id*., [0105]-[0112]. In the combination, the mobile phone of Hiroishi is configured to upload images to a remote terminal or server using HTTP, in a manner similar to what was suggested by Kahn. Also in the combination, Hiroishi sends a user preference that includes global positioning information as taught by Kahn. In addition, in the combination, Hiroishi displays an advertisement on the mobile application, as taught by Kahn.

1078. Also in the combination, the remote terminal of Hiroishi includes an authentication server to authenticate the user for accessing the remote terminal, as taught by Kahn. The remote terminal of Hiroishi in the combination also includes a database and a mobile software application advertising software module, as taught by Kahn.

1079. To the extent that Hiroishi's mobile phone and GUI are not interpreted to be a touch-based GUI, in the combination, Hiroishi's cellular phone uses a touch-based GUI, like that taught by Kahn.

1080. If necessary, in the combination, Hiroishi includes a timestamp signal sent from the digital camera to the mobile phone corresponding to the acquired new-data, as taught by Kahn.

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

1081. A POSITA at the time of the invention would have been motivated to combine the teachings of Hiroishi, Kahn, and Bluetooth, thus rendering the subject matter of the '381 patent Challenged Claims (claims 1-16) obvious.

1082. First, both Hiroishi and Kahn are analogous art to the claimed invention. Both references are from the same field of endeavor as the claimed invention: wireless image transfer from one electronic device to another. Hiroishi teaches techniques for enabling a mobile device to control a digital camera and transfer image files between and instructions between the two devices. *See, e.g.*, Hiroishi, Abstract, [0066]. Kahn is directed to wirelessly transferring image files from a mobile device to a publishing website over the Internet with an HTTP action setting. *See, e.g.*, Kahn, [0056], [0077] (describing the action setting of creating a new album on the server for uploading the images).

1083. Hiroishi and Kahn are both also pertinent to the problem of the '381

patent: transmission of image data by a cellular phone that was captured by a digital camera. TTI-1007, Background. Hiroishi addresses this problem through Bluetooth wireless data transmission and software-based control of the digital camera from the mobile device. *See, e.g.*, Hiroishi, [0043], [0053], [0061]. Kahn addresses the problem through efficient publishing of image data from a cellular phone to a website using HTTP. *See, e.g.*, Kahn, [0056], [0063].

1084. Second, a POSITA would have been motivated to use Kahn's upload technique to publish image data received at the mobile device of Hiroishi. At the time of the alleged Critical Date, photo-sharing websites and personal blogs had become ubiquitous. *See, e.g.*, TTI-1020, 3:25-49, 4:47-67; TTI-1021, 5:49-56 (describing use HTTP to send images from the phone to the server). Websites like FLICKR, PHOTOBUCKET, and PICASA allowed users to publish photographs and share them with friends, colleagues, and internet users. *See, e.g.*, TTI-1018, 5:25-28; TTI-1022, [0032].

1085. Cellular phones had also become ubiquitous. The original iPhone was released six months before the provisional filing date of the '381 patent (the iPhone was released on June 29, 2007), and years before that companies like Blackberry, Motorola, and Nokia had developed cellular phones that allowed users to transfer image data over the Internet. *See e.g.*, Hiroishi, [0015], [0047], FIG. 2. The '381 patent even refers to mobile phones as "ubiquitous." '381 patent, 10:21-22 ("The

mobile device 202 may, for example, be a **ubiquitous** mobile phone.") (emphasis added). Kahn also teaches a camera wirelessly connected to a mobile phone for capturing images and uploading images to a remote server. *See, e.g.*, Kahn, [0045], [0055]-[0057].

1086. Kahn recognizes both of these trends and teaches an efficient and predictable technique for uploading image data (captured by a camera) from a mobile device to a publishing website. *See, e.g.*, *id*., [0063].

1087. The teachings of Kahn would have provided straightforward benefit to the user of the mobile device in Hiroishi: predictable upload of image files and an action setting using an existing HTTP connection between the mobile device and a remote (publishing) server. Hiroishi already teaches the desire to transfer image data from a digital camera to a mobile device to a terminal device. *See, e.g.*, Hiroishi, [0044]. Kahn would have furthered this purpose by allowing the user to share image data over the Internet in a straight-forward and well-known way.

1088. Third, there would have been a reasonable expectation of success in combining the teachings of Hiroishi and Kahn. The combination would have required simply packaging the image data from the mobile device of Hiroishi in an HTTP message as Kahn teaches and as what was well known at the time for packet data transfer over the Internet. Both modifications would have been well within the ability of a POSITA. Doing so would have allowed the user to record the

images remotely using the well-known and efficient Internet transfer protocol of HTTP used by Kahn.

1089. Fourth, a POSITA would have been motivated, and found it obvious, to include user identifier that uniquely identifies a particular user of the Internet service. Hiroishi already teaches that the email address of the destination terminal is used to send images to the destination terminal. Hiroishi, [0110]. Because the '381 patent claims do not require that the user identifier uniquely identifies the operator of the mobile phone, Hiroishi alone would invalidate this feature. To the extent that the user identifier is interpreted to be the identifier of the user of the mobile phone, a POSITA would have found it obvious to include the user identifier with the images when transferring the images to the remote internet server. *See, e.g.*, Kahn, [0098]. This way, a POSITA would recognize the advantage of being able to uniquely identify the owner of the images, e.g., using a database field for user ID. Kahn, [0098]. In the example scenario of Hiroishi's print shop, the print shop worker can quickly and easily identify the owner of the images by the file name, and can validate the owner when providing the printed images. Likewise, the fulfillment center worker of Kahn can easily identify the owner of the images.

1090. A POSITA would have also been motivated to combine Hiroishi to include know the location ID of the camera sent with the images to the remote server, in a manner similar to that taught by Kahn. Hiroishi describes sending the

images from the phone to a print shop. *See, e.g.*, Hiroishi, [0049]. In the combination, a POSITA would have recognized the advantage of knowing current location information to identify a print shop (Kahn's fulfillment center) that was close by. *See, e.g.*, Kahn, [0094]. Furthermore, a POSITA would have known the advantage of including location information with the images would add to the later viewing enjoyment of the pictures by the location reminder of each photograph.

1091. A POSITA would have found it obvious to modify Hiroishi to include a time-stamp with the images, in a manner similar to that suggested by Kahn. As taught by Kahn, it was well known at that time (of the Kahn filing) that imaging devices recorded information about the date/time (timestamp) that an image was captured. Kahn, [0008]. This timestamp information provided information about when the images were captured. *Id*. In Kahn's system, the "image data already includes timestamp information (i.e., timestamp indicating when the image is captured)." *Id*., [0060]. Kahn explains that the timestamp information is useful for correlating timestamps with historical location information. *Id*. A POSITA implementing Hiroishi's system would have found it obvious to include the timestamp information, as was well known practice at the time, according to Kahn. *See, e.g.*, Kahn, [0008]. The timestamp information is also valuable so that images transmitted to remote servers could be organized by date. *See, e.g.*, Kahn, [0098]. A POSITA would have had a reasonable expectation of success implementing a

timestamp into the system of Hiroishi because including timestamp information into images recorded by digital cameras was a well-known practice at the time. Kahn, [0008].

1092. I note that the ’381 patent specification does not provide written description support for the camera (or other data capture device) sending a time-stamp to the mobile phone. At best, the ’381 patent describes the “segmentation module 203i [at the mobile phone] generates segment identifiers and tags the data segments with the segment identifiers. The segment identifiers may, for example, be one or more of transaction identifiers, sequence numbers, and timestamps.” ’381 patent, 8:26-30. While I believe that the transmission of a time-stamp from the camera to the phone with the images would have been an obvious modification to Hiroishi, the ’381 patent does not provide any written description support for doing so.

1093. A POSITA would have found it obvious that the remote terminals of Hiroishi would include a user software authentication module to authenticate the user of the cellular phone, as taught by Kahn. It would have been obvious to include such a server to store authentication credentials so that a user could securely access their remote image library, and so that the images stored on the remote image library could be secured from unauthorized accesses. Establishing such an authentication process would have been well within the abilities of a

POSITA at the time because authenticating a user for remote access to private information was a common and well known security tool at the time.

1094. A POSITA would have found it obvious to include a mobile client application advertising software module at the remote location, as taught by Kahn. As mentioned before, one of the terminals Hiroishi contemplates is a print shop, just like the fulfillment center of Kahn. In Kahn, the fulfillment center is identified based on global positioning information, so that fulfillment centers close to the user can be identified. It has already been established that a POSITA would have found it obvious to modify Hiroishi to also use global positioning information to likewise identify print shops that are close to the user. It would have also been obvious to include an advertisement software module to provide promotions and other advertisement information about nearby print shops / fulfillment centers to the user operating the program for uploading the images. *See, e.g.*, Hiroishi, [0122] (describing using a web browser to find nearby print shops). Doing so would have allowed the user to select a print shop / fulfillment center with good prices or coupons to save money. Likewise, the print shop or fulfillment center would earn business and make money by sending advertisements to the program of the cellular phone.

1095. A POSITA would have found it obvious to include a touch-based GUI in the combination. First, Hiroishi already teaches a touch-based GUI. *See, e.g.*,

Hiroishi, FIGS. 7A-D (describing a touch-based interactive graphical user interface for viewing and selecting images, and for transmitting images to a remote terminal). To the extent that touch-based GUI is interpreted to mean "touch screen" or the like, it would have been obvious to modify Hiroishi's touch-based GUI with a touch screen, like that described by Kahn. A POSITA would have known that touch screens were well known at the time for user interaction. A touch screen would have allowed the user in Hiroishi to easily select images on the screen for transmission. A POSITA would have also found it obvious to include touch-based advertisements on the touch-based GUI. A POSITA would have been motivated to include an easy way for the user to interact with advertisements presented on the touch-based GUI of Kahn.

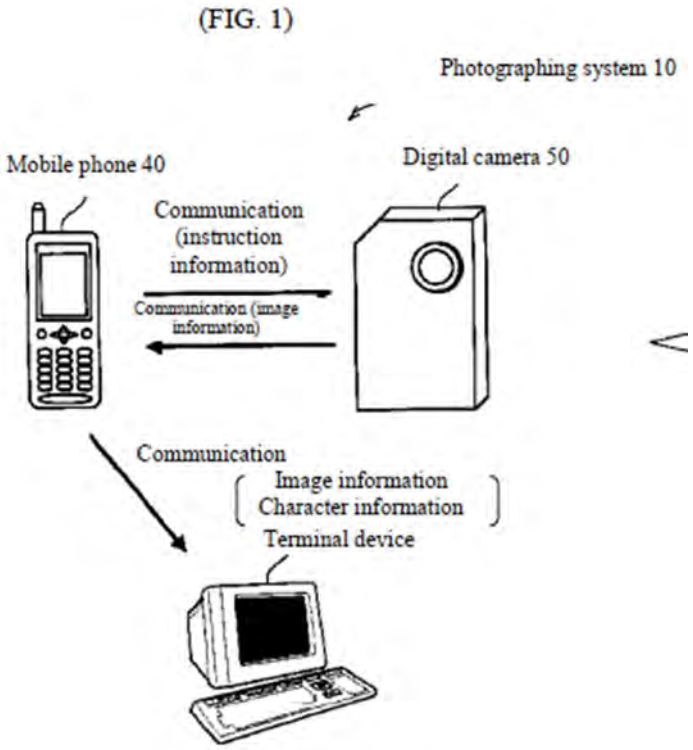
1096. Finally, because Hiroishi relies on Bluetooth, a POSITA would have been motivated to look to Bluetooth (e.g., the Bluetooth standard 2.1) for more information on the implementation and features of Bluetooth. To the extent that the Bluetooth features are not inherent or envisaged by a skilled artisan reading Hiroishi, it would have been obvious to use the details disclosed in Bluetooth with a system like Hiroishi, which states that Bluetooth is used for local wireless communication. In the combination, a POSITA would use the features disclosed in Bluetooth.

2. Analysis

[7.P] A mobile software application for a Bluetooth enabled cellular phone, wherein the mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, configured to:

1097. To the extent the preamble is limiting, the Hiroishi-Kahn-Bluetooth combination renders obvious [7.P]. Hiroishi teaches or suggests a mobile software application (a "program") for a Bluetooth enabled cellular phone embodied as executable instructions. For example, Hiroishi's system provides "a photographing system, a photographing method, a camera, a recording medium, and **a program** that allows the photographer him/herself to take a self-portrait reliably and to grasp the photographing timing correctly." Hiroishi, [0004] (emphasis added). Hiroishi teaches a digital camera device 50. Hiroishi, Fig. 1, Abstract ("[a] digital camera 50…."). Hiroishi further teaches a cellular phone 40 with access to the internet. *Id*. Fig. 2 (showing "mobile phone 40" connected to "Internet 12"), [0048], [0049]. Hiroishi further teaches that the digital camera is connected to the cellular phone over a wireless connection, such as Bluetooth. *Id*. [0066] ("The photographing system 10… is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth."), FIG. 1.

1098. In FIG. 1, Hiroishi illustrates a "basic configuration of the photographing system 10." Hiroishi, [0126].

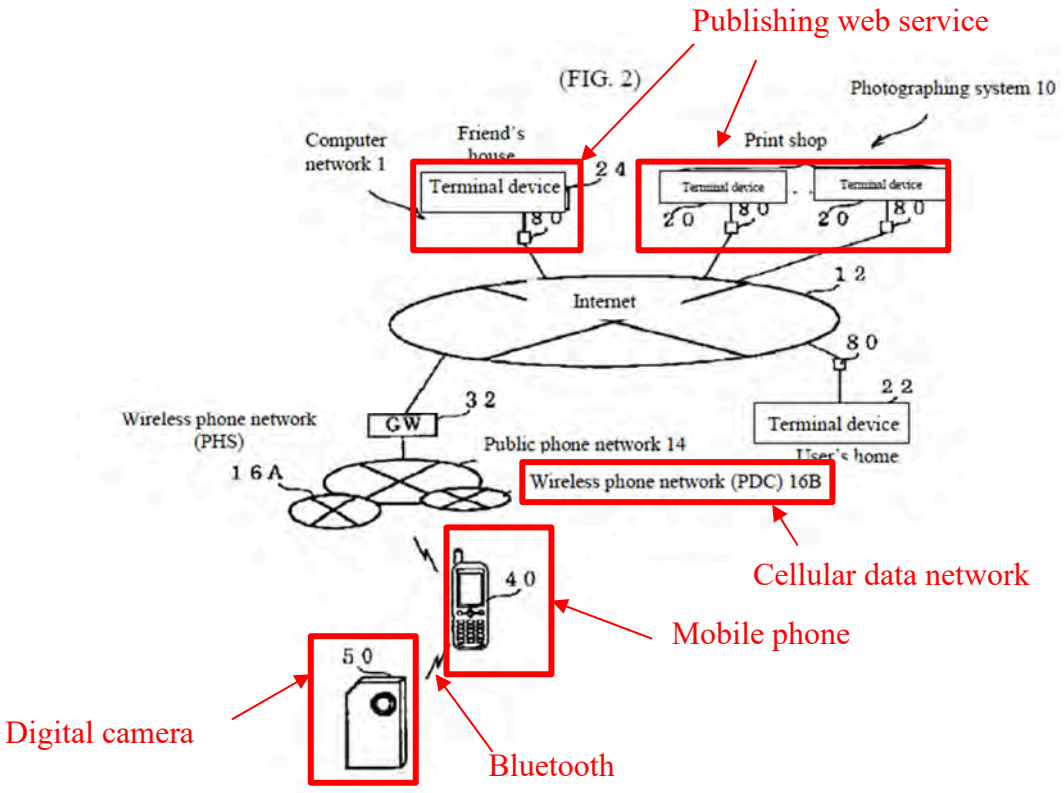


Hiroishi, FIG. 1.

1099. Hiroishi teaches that "the mobile phone 40 is configured so as to be mutually connected by a bus with a CPU (central processing unit) 41 that is responsible for the entire operation of the mobile phone 40; a ROM 42 for recording various control programs, parameters, and so forth; a RAM 43 used as a work area, or the like, at the time of execution of various control programs . . . ." Hiroishi, [0051].

1100. Hiroishi teaches a Bluetooth-enabled cellular phone (mobile phone 40) with cellular data capabilities to communicate over the Internet. TTI-1011, Fig. 2 (showing "mobile phone 40" connected to "Internet 12"), [0048]-[0049]. Hiroishi teaches a mobile phone 40 connected to a digital camera 50 using

Bluetooth. *Id.*, [0048]-[0049], [0066]-[0067], FIGS. 1-2. In FIG. 2, Hiroishi illustrates the photographing system. *Id.*, [0126].



Id., FIG. 1.

1101. Hiroishi teaches "[a] recording medium, capable of being read by a computer in which a program that controls the operation of a camera is installed." Hiroshi, Claim 10. A POSITA would have understood that Hiroishi's program would be alternative term for the mobile software application. A POSITA would have understood that the mobile phone 40 would have implemented a mobile software application to execute program (or set of instructions).

1102. Hiroishi lists the various instructions that the Bluetooth enabled

cellular phone can send to the digital camera over the Bluetooth connection to control the digital camera. Hiroishi, [0068]-[0069].

[7.1] detect and receive new-data acquired in a Bluetooth enabled data capture device

1103. *See, infra*, [7.3.1].]-[7.3.3]. This feature is broken up onto constituent components in the claim.

1104. Generally, Hiroishi teaches that new-data acquired by the camera (images captured and stored in camera memory) are "detected" when the mobile phone receives and the program running on the mobile phone displays thumbnail images representative of the images captured and stored in camera memory (new-data acquired). *See, e.g.*, Hiroishi, [0068], [0081]-[0082]. Later, the mobile phone receives the images captured by the camera and stored in camera memory (new-data acquired). *See, e.g.*, *id*., [0084], [0105]-[0106].

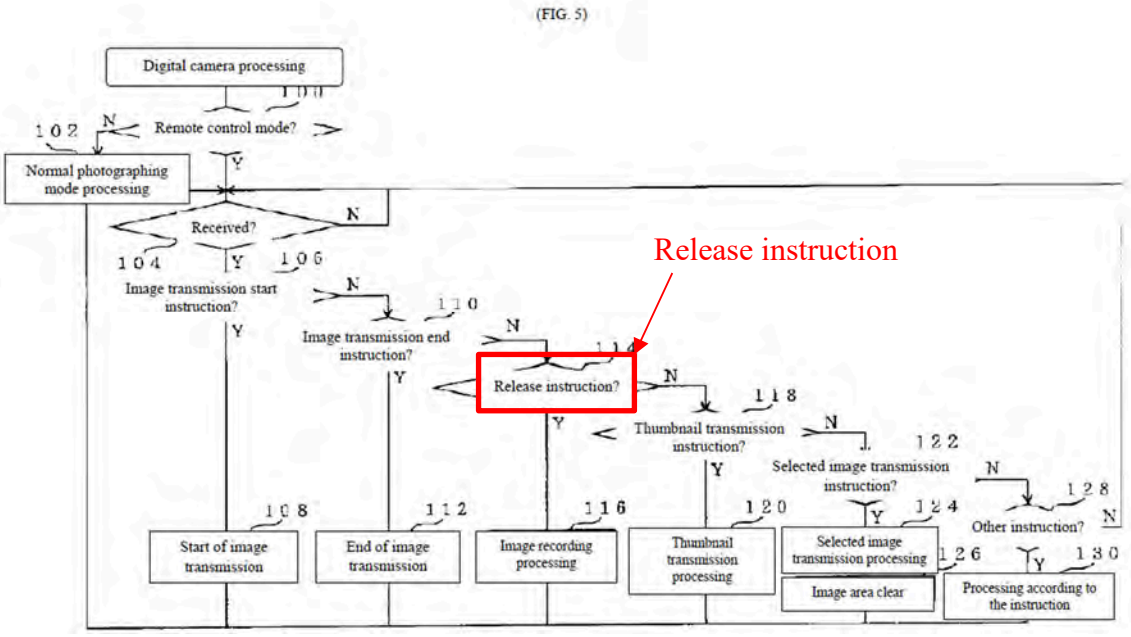
1105. In summary, a POSITA would have understood that Hiroishi detects new data acquired occurs when 1) the user sends a "release instruction" to the camera, resulting in the camera storing a captured image in its memory; 2) the user instructs the camera to end image transmissions; 3) the camera generates thumbnail images of the images stored in memory; and 4) the cellular phone receives the thumbnail images. The reception of the thumbnail images is the detection of new-data acquired.

[7.2.1] wherein the new-data is data acquired by the Bluetooth enabled data capture device after establishing a paired Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone,

1106. Hiroishi discloses "photographing system 10 …is configured so as to perform a two-way wireless communication between the mobile phone 40 and the digital camera 50 through Bluetooth… and can perform transfer of data signals." Hiroishi, [0066]-[0067]. The connection is paired because it allows two-way communication between the digital camera 50 and cellular phone 40. *Id*., [0066]. In FIG. 5, Hiroishi illustrates remote control of the digital camera by the cellular phone. Hiroishi, FIG. 5, [0071]-[0078]. In steps 100 and 104, the camera determines whether it is under remote control of the phone via the Bluetooth. *Id*.; *see also*, Hiroishi, [0070], [0074]-[0088], [0091]-[0107], [0121].

1107. Generally, Hiroishi teaches that the mobile software application is configured to detect new data upon receipt of thumbnail images from the camera. In operation, the camera of Hiroishi continuously sends images to the mobile phone. Hiroishi teaches that the program on the mobile phone sends a "release instruction" from the mobile (or cellular) phone to the digital camera 50 after establishing a Bluetooth connection between the camera and the phone. *See, e.g.*, Hiroishi, Abstract, [0012]. Hiroishi emphasizes that "the release instruction information is the information for instructing the timing of photographing with the camera of the present invention." Hiroishi, [0034]. The release instructions from

the mobile phone would allow the camera "to photograph a picture … by transmitting the release instruction information at the timing one wishes to take a photograph with the camera of the present invention. Therefore, since the timing in which the release instruction information is transmitted serves as the photographing timing, the photographer can grasp the photographing timing correctly." *Id*., [0034].



Hiroishi, FIG. 5.

1108. As shown above in FIG. 5, Hiroishi illustrates remote control of the digital camera by the cellular phone. Hiroishi, FIG. 5, [0071]-[0078]. In steps 100 and 104, the camera determines whether it is under remote control of the phone via the Bluetooth. *Id*. At step 114, the camera receives a release instruction from the phone causing it to acquire a new image. Id., Abstract ("the mobile phone 40…

transmits the release instruction information to the digital camera 50"), [0034] ("it is possible to photograph a picture with a camera also at the position away from the camera, by transmitting the release instruction information at the timing one wishes to take a photograph with the camera"), [0078] ("In Step 114, a determination is made as to whether the instruction information received in Step 104 is the release instruction information…."). A POSITA would understand that, because the release instruction is received from the phone over the Bluetooth connection, the image is acquired after the wireless connection is established. *Id*.

[7.2.2] wherein establishing the Bluetooth paired connection comprises the Bluetooth enabled data capture device cryptographically authenticating an identity of the Bluetooth enabled cellular phone,

1109. First, Hiroishi teaches that the mobile phone and the camera are linked via a Bluetooth connection. *See, e.g.*, Hiroishi, [0066]-[0067]. For the mobile phone and the camera to communicate via Bluetooth, the mobile phone and the camera must have been "paired." *See, e.g.*, Bluetooth Core Specification V2.1, 412 (4.2.2 Pairing), 131 (5 Secure Simple Pairing Overview). The Bluetooth Core Specification V2.1 uses cryptographic authentication as part of the Bluetooth pairing process. *Id*. For example, the Bluetooth Specification V.2.1 + EDR [Vol 2] describes authentication procedures. Specifically, the pairing process includes the exchange of BD_ADDR, which is a Bluetooth device identifier, along with an initialization key and PIN:

4.2.2 Pairing

When two devices do not have a common link key an initialization key (K_{init}) shall be created using either the pairing or Secure Simple Pairing procedures. When pairing is used, K_{init} shall be created based on a PIN, and a random number and a BD_ADDR. K_{init} shall be created as specified in [Part H] Section 6.3 on page 885. When both devices have calculated K_{init} the link key shall be created, and a mutual authentication is performed. The pairing procedure starts with a device sending an LMP_in_rand PDU; this device is referred to as the "initiating LM" or "initiator" in Section 4.2.2.1 on page 242 - Section 4.2.2.5 on page 245. The other device is referred to as the "responding LM" or "responder". The PDUs used in the pairing procedure are:

M/O	PDU	Contents
M	LMP_in_rand	random number
M	LMP_au_rand	random number
M	LMP_sres	authentication response
M	LMP_comb_key	random number
M	LMP_unit_key	key

Table 4.14: Pairing PDUs

All sequences described in Section 4 on page 223, including the mutual authentication after the link key has been created, shall form a single transaction. The transaction ID from the first LMP_in_rand shall be used for all subsequent sequences.

See, e.g., Bluetooth Specification V2.1, 412.

1110. The BD_ADDR is the address of the Bluetooth device, which is a unique identifier. In this way, the cryptographic authentication authenticates the identity of the mobile phone.

1111. To the extent that the Patent Board finds that cryptographically authenticating the identity of the mobile device is not inherent by the use of Bluetooth, it would have been obvious at the time to cryptographically authenticate the identity of the mobile phone by the camera in order pair the mobile phone with the camera to securely establish the Bluetooth connection.

1112. Cryptographic authentication between wireless devices like a digital

camera and cellular phone communicatively coupled via Bluetooth was routine at the time of the alleged Critical Date. It is my opinion that it would have been obvious to a POSITA at the time of the invention to modify Hiroishi to include this feature because Hiroishi does teach using Bluetooth as the standard for communications between the mobile phone 40 and the camera 50. *See, e.g.*, Hiroishi, [0066]-[0067].

1113. In my opinion, a POSITA also would have found this benefit directly applicable to the digital camera and cellular phone system disclosed Hiroishi, because it would have ensured the secure transmission of image files and related data between the two devices. Hiroishi teaches that the digital camera and cellular phone implement a "predetermined communication protocol" and identifies Bluetooth as the preferred data transmission mechanism, so there would not have been any unexpected result if the digital camera and cellular phone were configured to cryptographically authenticate each other. Hiroishi, [0049]-[0052], [0058].

[7.3.1] wherein detecting and receiving new-data acquired in the Bluetooth enabled data capture device comprises: said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection,

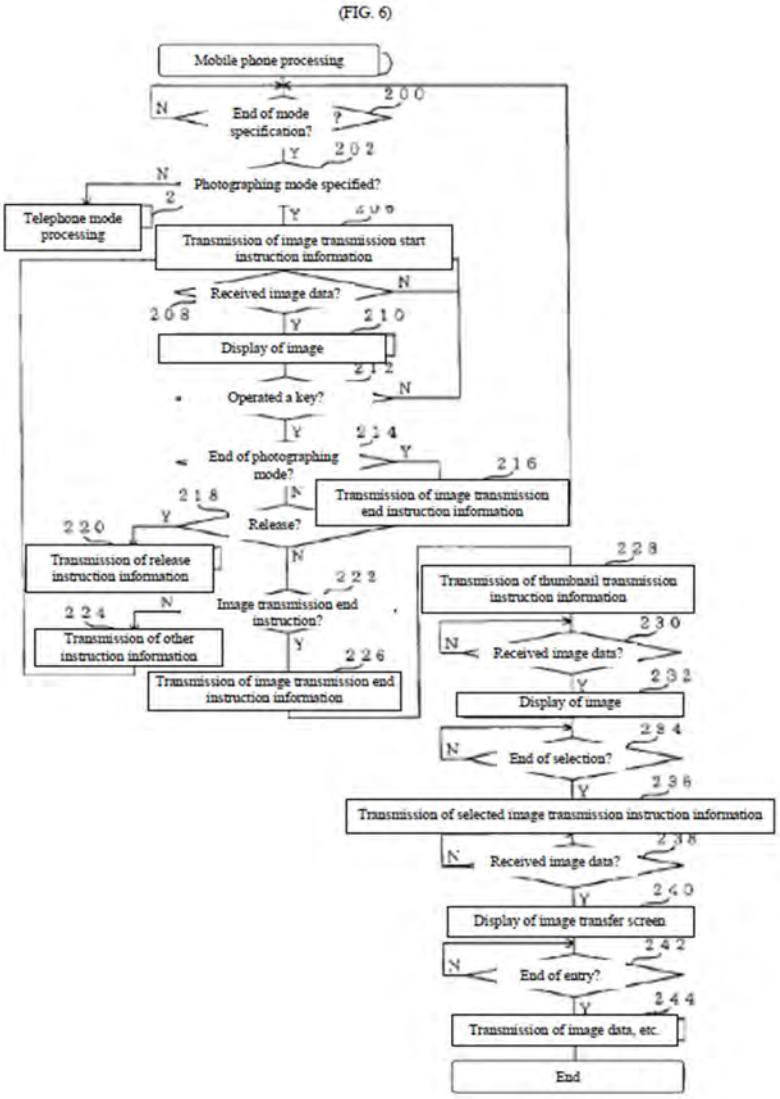
1114. Hiroishi-Kahn-Bluetooth renders [7.3.1] obvious. In the combination, Hiroishi's program is configured to wait for response (listen) for a

thumbnail image (an event notification) from the camera over the Bluetooth connection. TTI-1011, [0081]-[0082], [0104]-[0105].

1115. In the claim, the cellular phone detects and receives new data by listening for an event notification signal. The signal informs the cellular phone that new data is available. In the Hiroishi-Khan combination, there are a variety of signals that would perform the event notification function. For example, Hiroishi sends thumbnails to the cellular phone. Upon receipt of the thumbnails, the cellular phone is notified that the pictures represented by the thumbnails are available. In addition, it would have been obvious to include header information, metadata, or some other information with the thumbnails or in addition to the thumbnails that informs the cellular phone of the nature of the received data—that new photos are available. A person of ordinary skill would have reason to provide an event notification or designate pre-existing data as an event notification so that the cellular phone is made aware that new data is available so that it may then take appropriate actions in response. Because thumbnails provide a straight-forward event notification to the user, a person of ordinary skill would further use the thumbnails or associated metadata identifying the thumbnails as thumbnails as an event notification in the software running on the cellular phone.

1116. A POSITA would have understood that the program on the mobile phone "waits" for the thumbnail images, the waiting constituting as the phone

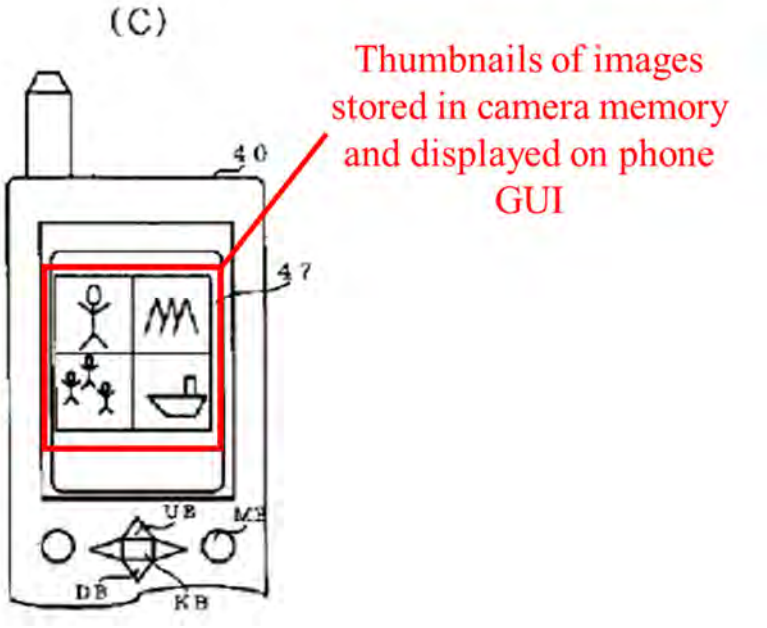
listening for the event notification signal. *See, e.g.*, TTI-1011, [0104].



TTI-1011, FIG. 6.

1117. The camera performs "thumbnail transmission ... and the image data for displaying thumbnails is transmitted to the mobile phone 40." *Id.*, [0102]. During this time, the phone "waits until it receives the image data that can display the thumbnail from the digital camera 50, and in the following Step 232, after a decompression process is performed to the received image data, the thumbnail

shown according to the image data is displayed on the display unit 47 [of the phone]." *Id.*, [0104].



Id., FIG. 7(c) (annotated).

1118. The thumbnails correspond to the acquired new data (the image captured by the camera and stored on the camera memory when the release instruction is given). The "image data that can display thumbnails is created by performing a predetermined image processing to the digital image data stored in the photographed image data storage area of SDRAM 55A (not shown), a thumbnail transmission processing for transmitting the image data to the mobile phone 40 is performed, and the process returns to Step 104 thereafter." TTI-1011, [0081]-[0082].

1119. Accordingly, Hiroishi teaches that the mobile phone's program is configured to listen (waits) for an event notification (thumbnail images).

1120. In addition, or in the alternative, Kahn teaches the program (applet) configured to listen for an event notification. For example, Kahn teaches that the user selecting an upload or upload all button on the phone's GUI causes images on the camera to be transferred to the server. *See, e.g.*, TTI-1017, FIG. 5B. A POSITA would have understood that when the user selects upload/upload all, the phone would have had to start listening for a signal from the camera. In Kahn, the images include a timestamp. *See, e.g.*, TTI-1017, [0008], [0060]. The '381 patent fails to describe what the event notification is.[3] Thus, a POSITA reviewing the '381 patent family would have turned to other intrinsic evidence to understand what the event notification was. According to the '030 patent, which shares the same specification and priority claim, the data signal notification can include timestamp attribute inside the data object. *See, e.g.*, TTI-1001, Claim 6. A POSITA reviewing the '381 patent family would have recognized that a timestamp was an event notification from claim 6 of the '030 patent.

1121. In addition, or in the alternative, Hiroishi's use of Bluetooth satisfies element [7.3.1]. Specifically, Bluetooth teaches polling. *Id*.; TTI-1019, 332.

[3] The '381 patent specification does not use the term "event notification."

[7.3.2] wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone; and

1122. The Hiroishi-Kahn-Bluetooth combination renders obvious [7.2]. In my opinion, Hiroishi-Kahn-Bluetooth teaches a mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection, wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone.

1123. As discussed above, a POSITA would have also understood that the thumbnails being sent to the phone from the camera constitute the signal representing the event notification.

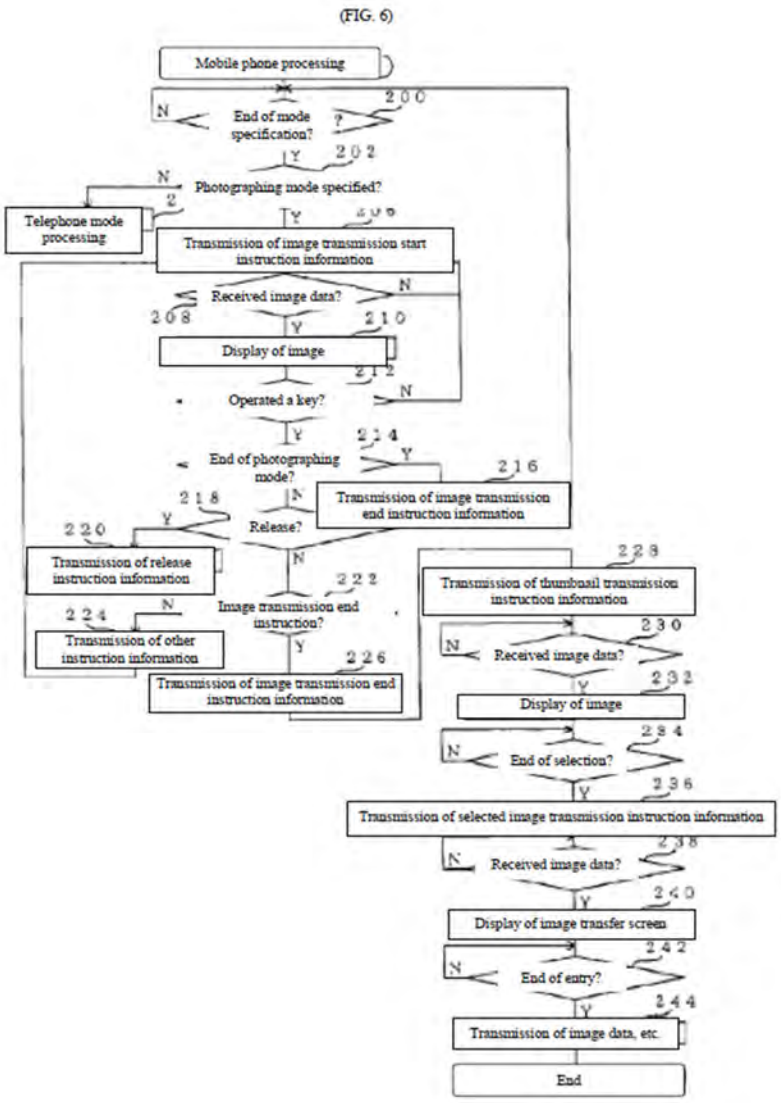
1124. In operation, after the camera of Hiroishi captures and stores an image, the user of the mobile phone can request thumbnails of the images stored in the camera memory. Hiroishi, [0068], [0081]-[0082]. The camera creates thumbnails from images stored in memory. *Id*., [0082]. The camera then sends the thumbnails to the mobile phone for display to the user on the program's user interface. *Id*., [0081]-[0082], [0084], [0102].

1125. The thumbnails (event notification) created by the camera represent (i.e., correspond to) the full resolution images captured (new-data acquired) by the

camera. A POSITA, therefore, would recognize the thumbnails received by the mobile phone and displayed to the user on the program constitute a signal sent from the camera to the mobile phone. In addition, or in the alternative, the timestamp described in Kahn is used in the combination as an event notification because it is a signal that "corresponds to the acquired new-data." See, e.g., id., [0066]-[0067]; TTI-1017, [0008] (describing "prior art imaging devices have only been able to record information about date/time (timestamp) that an image was captured"), [0060] (describing that "the image data already includes timestamp information (i.e., timestamp indicating when the image is captured" (emphasis added)); See Ground 1, Claim, [7.3.1]. The timestamp is the signal of element [7.3.2] because it is in the image data that is sent from the camera to the phone during the upload to the server. Id. And, as mentioned, the timestamp corresponds to when the image is captured, making it unique to each image. TTI-1017, [0008], [0060].[7.3.3] said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection,

1126. For example, Hiroishi teaches "[a] recording medium, capable of being read by a computer in which a program that controls the operation of a camera is installed." Hiroshi, Claim 10. A POSITA would have understood that Hiroishi's program that runs on the mobile (or cellular) phone is a mobile software

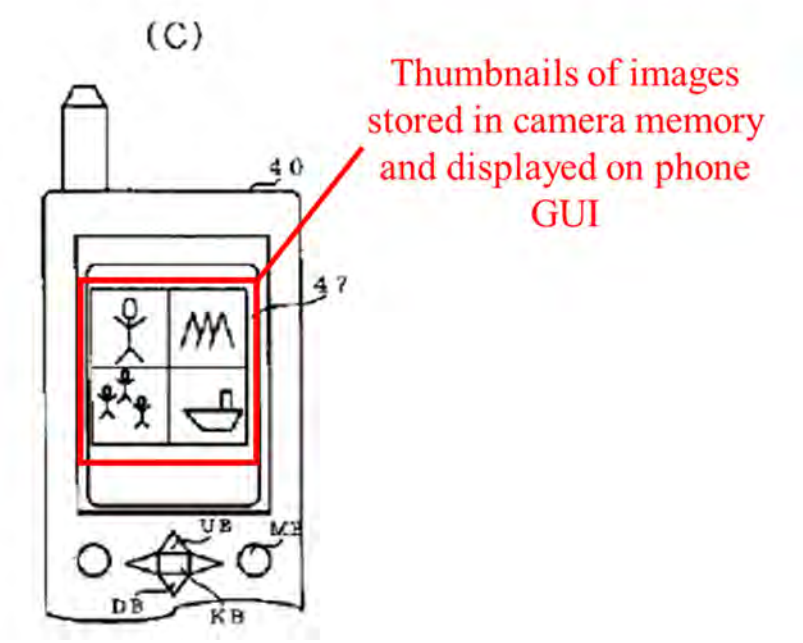
application. The program (mobile software application) is configured to wait for response (listen) for a thumbnail image (an event notification) from the camera over the Bluetooth connection, wherein the thumbnail (event notification) corresponding to the acquired full resolution image (new-data) and comprises sending a thumbnail over Bluetooth connection from the camera to the phone. Hiroishi, [0081]-[0082], [0104]-[0105]. A POSITA would have understood that the phone's (and/or program installed on the phone. Hiroishi, Claim 10, Abstract) "wait" action for the thumbnail images, constitutes as the phone listening for the event notification signal. *See also*, Supra [7.1].



Hiroishi, FIG. 6.

1127. As shown above in FIG. 6, Hiroishi discloses after sending a request to the digital camera, the cellular phone "waits" for the image data in response. Hiroishi, [0102]-[0104]. Subsequently, the camera performs "thumbnail transmission… and the image data for displaying thumbnails is transmitted to the mobile phone 40." Hiroishi, [0102]. During this time, the phone "waits until it receives the image data that can display the thumbnail from the digital camera 50,

and in the following Step 232, after a decompression process is performed to the received image data, the thumbnail shown according to the image data is displayed on the display unit 47 [of the phone]." Hiroishi, [0104].



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

1128. The thumbnails correspond to the acquired new data (the image captured by the camera when the release instruction is given). The "image data that can display thumbnails is created by performing a predetermined image processing to the digital image data stored in the photographed image data storage area of SDRAM 55A (not shown), a thumbnail transmission processing for transmitting the image data to the mobile phone 40 is performed, and the process returns to Step 104 thereafter." Hiroishi, [0081]-[0082].

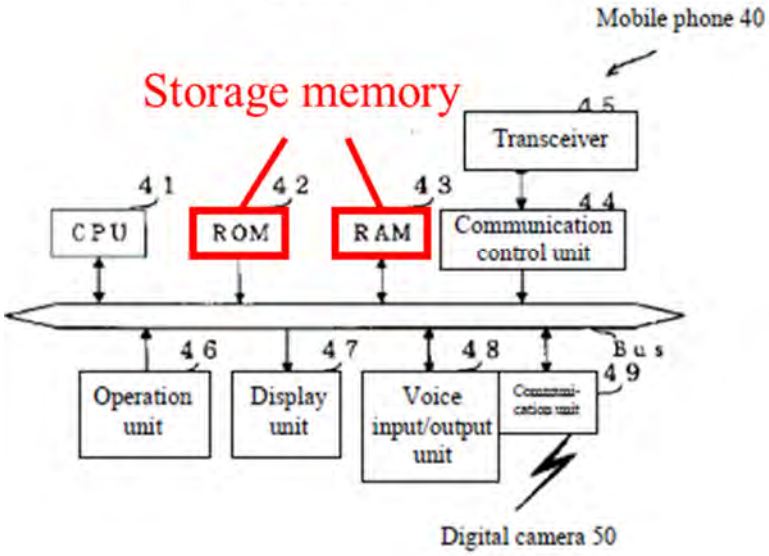
1129. The Hiroishi-Kahn-Bluetooth combination renders obvious [7.3]. Hiroishi-Kahn-Bluetooth teaches mobile software application for the Bluetooth enabled cellular phone configured to receive, from the Bluetooth enabled data capture device, the event notification and the acquired new-data over the established paired Bluetooth connection. As discussed above, Hiroishi's program (mobile software application) is configured to receive, from the camera, the thumbnail (event notification) and the acquired full resolution image (new-data) over the established Bluetooth connection. Supra [7.P], [7.2]. See also, Hiroishi, claim 10, [0066]-[0068], [0121]. In addition, or in the alternative, Kahn teaches that the timestamp is included in the image data that is sent from the camera to the mobile phone. See, e.g., TTI-1017, [0008], [0060]; See Ground 1, Claim [7.3.1]-[7.3.2]. Thus, the event notification (timestamp) and acquired new-data (full resolution images) are received by the mobile phone. In the combination, a POSITA would use the timestamp as a notification that images are available for uploading.[7.4] store the received new-data in a memory of the Bluetooth enabled cellular phone;

1130. The Hiroishi-Kahn-Bluetooth combination renders obvious [7.4]. In my opinion, Hiroishi-Kahn-Bluetooth teaches storing the received new-data in a memory of the Bluetooth enabled cellular phone. Hiroishi teaches that a user may access the camera from the cellular device and select image files to be transmitted

to the cellular device over the Bluetooth connection.

1131. The cellular phone in Hiroishi clearly stores a new-media file received from the digital camera, because after receiving the new-media file, the cellular phone can then send the file to a further destination. Hiroishi, FIG. 6, [0108] ("FIG. 7(D) shows the image transfer screen displayed on the display unit 47… for entering the information showing the desired transfer destination to transmit the digital image data…."), [0078], [0084].

(FIG. 3)



Hiroishi, FIG. 3 (annotated)

1132. As shown in FIG. 3 above, Hiroishi teaches that the cellular phone includes both ROM 42 and RAM 43 memory storage devices. Hiroishi, FIG. 3, [0051]. A POSITA would understand that the received new-data images could be stored in either ROM 42 or RAM 4, but would recognize that storing them in non-

volatile memory would be advantageous so that the images are not lost in the case of power lost. A POSITA would know that a true ROM cannot be written, as it is read only memory. Hiroshi indicates that the ROM has 2 regions, one for the executable program instructions for the CPU 41 and another one for the images, [0088], ("Therefore, the digital camera processing program represents the program of the present invention, and ROM 55B represents the recording medium of the present invention.") so a POSITA would understand that Hiroishi's ROM device is not really a read only memory, but rather a non-volatile memory at the time of the patent priority date like a Flash memory (or similar) where some or all sections could be written in circuit (not read only) and furthermore would not be lost if the power to the mobile phone 40 was lost.

1133. In light of these teachings, a POSITA would have been motivated to use the non-volatile memory on the cellular phone as a predictable location to store new-media files received from the digital camera.

[7.5] 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

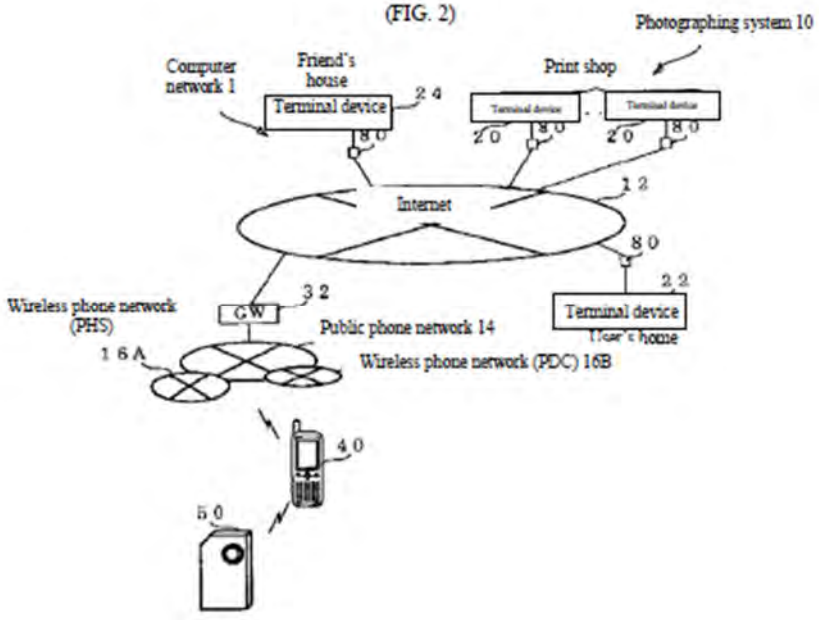
1134. The Hiroishi-Kahn-Bluetooth combination renders obvious [7.5]. Hiroishi-Kahn-Bluetooth combination teaches use Hypertext Transfer Protocol to transfer the received new-data along with a user authentication credential to a

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.

1135. This limitation is broken down into constituent steps below:

[7.5.1] 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

1136. For example, Hiroishi teaches that the cellular phone is configured to upload the received new-media file to a "terminal" via the internet. Hiroishi, Fig. 2, [0044] ("the mobile phone 40 forwards the image information received from the digital camera 50 to a terminal device").



Hiroishi, FIG. 2.

1137. Furthermore, as an example Hiroishi discloses that "[m]utual access of the terminal unit 20, the terminal unit 22, the terminal unit 24, and the mobile phone 40 on such a network [i.e. network 12] is possible according to a predetermined communication protocol, such as TCP/IP (Transmission Control Protocol/Internet Protocol)," Hiroishi, [0049].

1138. In one instance, Hiroishi's program (mobile software application) is further configured to send (via email) a user preference (e.g., the number of sheets to be printed and the scheduled pick-up date and time specifying the terminal unit 20 of a print shop) to the remote server (the email server of the print shop) over the cellular data network. Hiroishi, [0110]. Because Hiroishi teaches sending an email, the email address of the sender would have been included in the email. The email address of the sender constitutes a user authentication credential.

1139. Given the widespread use of HTTP, a POSITA would have understood that Hiroishi's mobile phone would have implemented communication with network 12 using HTTP. Specifically, it would have been obvious for Hiroishi's phone application to use HTTP (webmail) to transfer the received new-data (full resolution image) along with a user authentication credential (email address of the sender/phone application user) to a remote server (e.g., an email server hosting the email address of the terminal unit of the transfer destination) over a cellular data network (Hiroishi's cellular data network). For example,

Hiroishi teaches that the user of the phone can send the images to a remote server by sending the photos via e-mail. Hiroishi, [0110] ("When such an image transfer screen is displayed on the display unit 47, an operator enters the information showing the transfer destination of the digital image data received in Step 238 (according to this embodiment, an e-mail (electronic mail) address of the terminal unit of the transfer destination) and the number of sheets to be printed and the scheduled pick-up date and time specifying the terminal unit 20 of a print shop as the transfer destination using the numeric keypad (not shown) or the like, provided on the mobile phone 40 within the corresponding rectangular frame."), [0122]

1140. Hiroishi-Kahn-Bluetooth teaches about uploading (***publishing***) media content (***data***) on online service provider (***online data publishing web service***).

1141. However, a POSITA would have found it obvious to use HTTP methods for an action setting. Given the widespread use of HTTP, a POSITA would have understood that Hiroishi's mobile phone would have implemented communication with network 12 using HTTP. Specifically, it would have been obvious for Hiroishi's phone application to use HTTP (webmail) to transfer the received new-data (full resolution image) along with a user authentication credential (email address of the sender/phone application user) to a remote server (e.g., an email server hosting the email address of the terminal unit of the transfer destination) over a cellular data network (Hiroishi's cellular data network).

[7.5.2] 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

1142. Referring to FIG. 1, Hiroishi's phone application is further configured to send (via email) a user preference (e.g., the number of sheets to be printed and the scheduled pick-up date and time specifying the terminal unit 20 of a print shop) to the remote server (the email server of the print shop) over the cellular data network.

1143. As explained above (supra [7.5.1]), it would have been obvious to use HTTP (GMAIL) to send those user preferences. It also would have been obvious in view of Kahn to send GPS information. Kahn teaches transmitting a user preference including location information from GPS component, Kahn, [0062] ("user wishes to upload images to the user's account on an image server. The upload program 410 is also invoked… The upload program 410 communicates with the location API 420… that provides an API to the GPS module (e.g., for embodiment having a GPS module embedded within the host/cell phone device)."), id., [0097] ("user manually requests uploading… upon receipt of the request that the images be uploaded, a local application (applet) is invoked that associates location information with the images. This includes the following sub steps. First, the applet submits a query to the GPS module to return a location ID comprising the current position (latitude and longitude). Next, the applet transmits

this location ID to the image manager, as part of the transmission that uploads the images."). See also, Kahn, [0098] ("Upon receipt of the transmission from the applet, the image manager proceeds to store the images (in an image server) and stores the location ID information in the metadata database… the images are stored as individual files (e.g., using UNIX file system). 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, time-stamp (date/time), and location ID (longitude and latitude decimal values)."). A POSITA would have been motivated to include GPS information for the reason stated in Kahn – to enable the media content to be geotagged or geocoded.

[7.6] display a mobile advertisement inside the mobile software application.

1144. The Hiroishi-Kahn-Bluetooth combination renders obvious [7.6]. Hiroishi-Kahn-Bluetooth teaches display a mobile advertisement inside the mobile software application. For example, Kahn teaches displaying promotion on the user's device, particularly, "promotions that are relevant to that user location." Kahn, [0087]. Kahn teaches about "location information" being "used to offer location-dependent promotions to the user." Kahn, [0051].

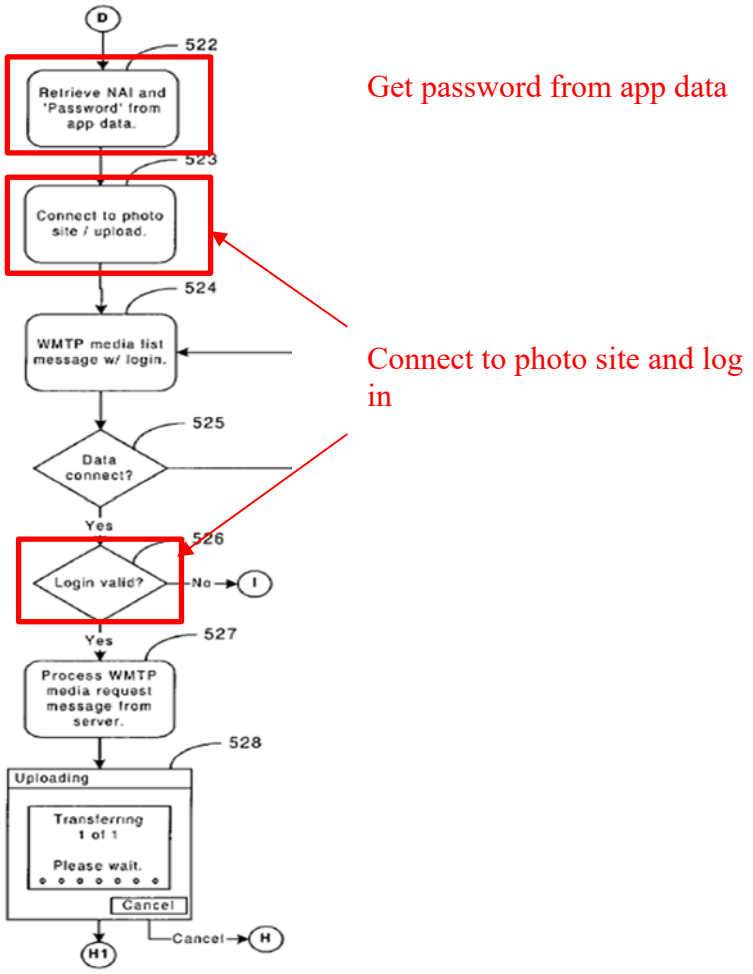
1145. A POSITA would have been further motivated to include GPS information for the reason stated in Kahn – to offer location-dependent promotions

to the user. Kahn at [0051].

1146. Also see *infra* [11] showing another disclosed advertising example.

[8] The mobile software application of claim 7, wherein the user authentication credential is stored in the memory of the Bluetooth enabled cellular phone, and wherein the user authentication credential is used by the remote server to authenticate a user.

1147. Hiroishi-Kahn-Bluetooth renders obvious Claim [8]. In the combination, Kahn teaches the user authentication credential is stored in the memory of the Bluetooth enabled cellular phone, and wherein the user authentication credential is used by the remote server to authenticate a user. *Id*. For example, Kahn teaches "the applet retrieves the network access identifier or NAI (e.g., user cell phone number) and password." TTI-1017, [0071]. The password is stored in application data, on the mobile phone, and is used as a credential for accessing the photo site for uploading. *See, e.g.*, *id*., FIG. 5C. FIG. 5C is shown below:



Id., FIG. 5C (partial, annotated).

1148. Kahn also teaches a database that includes a database table that 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)." *Id.*, [0098].

[9] The mobile software application of claim 7, wherein the remote server is configured to store the new-data.

1149. Hiroishi-Kahn-Bluetooth renders obvious Claim [9]. *See also supra* [7.5]. In the combination, Hiroishi teaches the remote server is configured to store

the new-data. *Id*. For example, Hiroishi teaches storing the images at a remote server, such as a friend's terminal or the user's terminal; and at least temporarily, the images would have been stored in the print shop terminal. *See, e.g.*, TTI-1011, [0114] (describing that "the digital image data received from the mobile phone 40 is stored in a predetermined area of a built-in storage device (not shown) in the terminal unit 22 or the terminal unit 24."); *see also id*., [0111]-[0112] (describing print shop receiving and inherently storing the images).

1150. To the extent that Hiroishi is interpreted to not teach the features of claim 9, Kahn so teaches. For example, Kahn teaches image servers for storing images received from the mobile phone. *See, e.g.*, TTI-1017, [0056], [0064], [0098]. It would have been obvious to a POSITA to store the images in a remote image server, as taught by Kahn, so that the images could be viewed, downloaded, printed (fulfilled) at the user's discretion without taking up local storage on the mobile phone or camera. In addition, it would have been obvious to store the images prior to fulfillment at the print shop or fulfillment center so that the images could be edited and/or printed. *See, e.g.*, *id*.; TTI-1017, [0068]; TTI-1011, [0111]-[0112].

[10] The mobile software application of claim 7, wherein the mobile software application provides a touch based GUI for the received new-data.

1151. The Hiroishi-Kahn-Bluetooth combination renders obvious [10]. Hiroishi-Kahn-Bluetooth teaches the mobile software application provides a touch

based GUI for the received new-data.

1152. For example, Kahn discloses "user interface (UI)." *See, e.g.*, TTI-1017, [0025], FIGS. 5A-E. Kahn discloses "a Palm PDA device ... with wireless connectivity (e.g., Palm i705).").[4] *Id*., [0045]. A POSITA would have recognized that Palm i705 comprises touch based GUI. see, e.g., TTI-1029, [0025, [0089], [0091].

1153. As shown in FIGS 5A-E, Kahn presents interactive buttons that are displayed on the GUI:

[4] Shiigi discloses "The handwriting or handdrawing input device can be a touch screen." TTI-1029, [0025]. Shiigi also teaches that the "handwritten input can be entered with a touch pen." *Id*. [0089]. Further, an example Shiigi gives for the touch screen device is "Palm's announced i705 wireless device". *Id*. [0091].

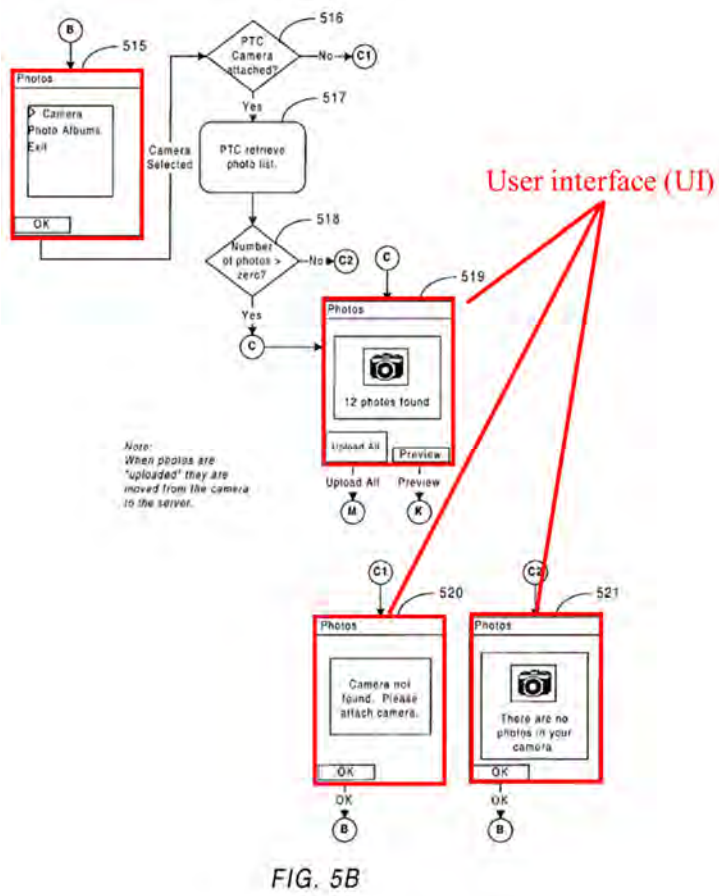
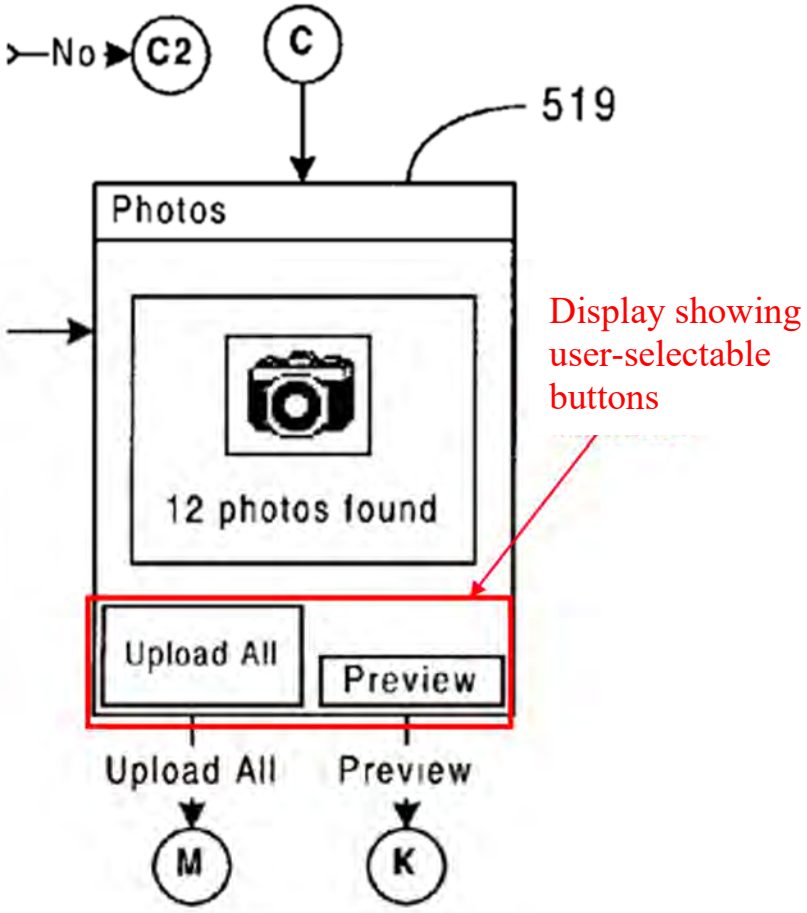


FIG. 5B

TTI-1017, FIG. 5B (annotated).

1154. For example, Kahn discloses a user interface flow diagram showing the display (GUI) on the host device 300 application that is controlling camera 310 in FIGs. 5A-5F that includes buttons such as a Preview button in screen 519 on FIG. 5B, that allows the viewing of pictures ("for the received new data") via "K", the circle flowchart symbol leading to screen 550 on FIG. 5E showing the selected received new data picture on the GUI. TTI-1017, [0025], [0055], FIGs. 5B and 5E.



1155. FIG. 5B (excerpt) showing GUI.

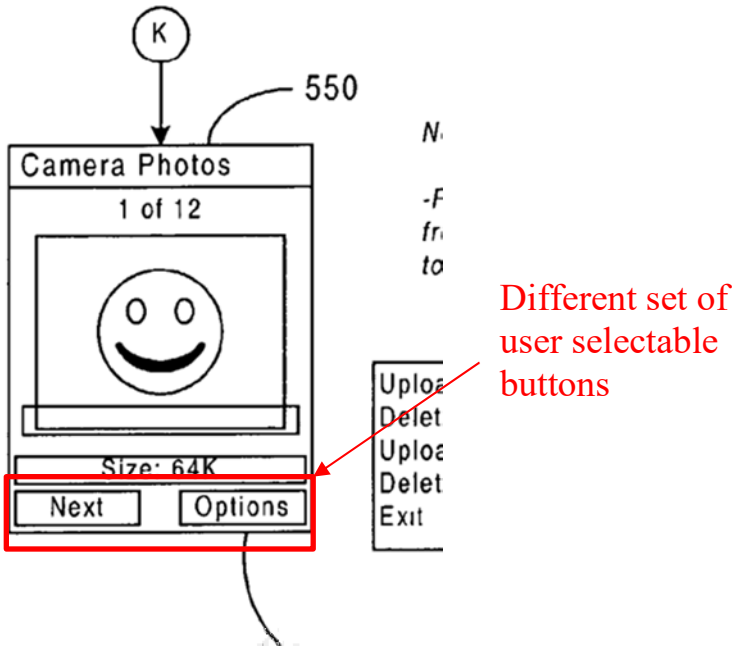


FIG 5E (excerpt) showing GUI.

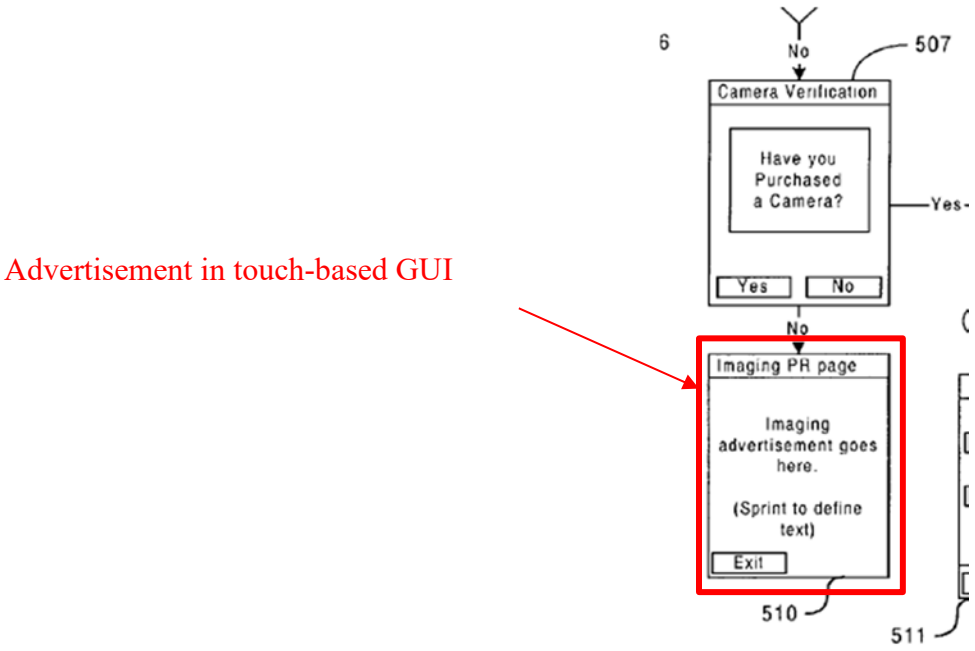
1156. Furthermore, Kahn discloses a mobile phone involving touch based GUI, Kahn, [0045] ("the digital camera 100 would occasionally be connected to a local host device, such as a cellular phone or a Palm PDA device (available from Palm, Inc. of Santa Clara, Calif.) with wireless connectivity (e.g., Palm i705)."). Shiigi confirms that the Palm i705 has a touch based graphical user interface.[5]

1157. Based on the examples provided, a POSITA would have understood that Kahn discloses mobile software application provides a touch based GUI for the received new-data.

[5] Shiigi discloses "The handwriting or handdrawing input device can be a touch screen." TTI-1029, [0025]. Shiigi also teaches that the "handwritten input can be entered with a touch pen." *Id*. [0089]. Further, an example Shiigi gives for the touch screen device is "Palm's announced i705 wireless device." *Id*. [0091].

[11] The mobile software application of claim 7, wherein the mobile software application provides a touch based advertisement targeted to a user.

1158. Hiroishi-Kahn-Bluetooth renders obvious Claim [11]. *See also supra* [7.6] and [10]. In the combination, Kahn teaches that advertisements and promotions are displayed on the touch-based GUI, e.g., a WAP Page. *See, e.g.*, TTI-1017, [0087], FIG. 5A:



Id., FIG. 5A (annotated, partial)..

[1.P]-[1.1] A system, comprising: a mobile software application for a Bluetooth enabled cellular phone, wherein the mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, configured to:

1159. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.P]-[1.1]. Supra [7.P].

[1.2]-[1.3.2] detect and receive new-data acquired in a Bluetooth enabled data capture device, wherein the new-data is data acquired by the Bluetooth

enabled data capture device after establishing a paired Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone, wherein establishing the Bluetooth paired connection comprises the Bluetooth enabled data capture device cryptographically authenticating an identity of the Bluetooth enabled cellular phone, wherein detecting and receiving new-data acquired in the Bluetooth enabled data capture device comprises:

1160. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.2]-[1.32]. Supra [7.1]-[7.3.1].

[1.4.1]-[1.4.2] said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection, wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone; and

1161. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.4.1]-[1.4.2]. Supra [7.3].

[1.4.3] said mobile software application for the Bluetooth enabled cellular phone configured to receive, from the Bluetooth enabled data capture device, the event notification and the acquired new-data over the established paired Bluetooth connection;

1162. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.4.3]. Supra [7.3].

[1.5] store the received new-data in a memory of the Bluetooth enabled cellular phone;

1163. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.5]. Supra [7.4].

[1.6.] 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

1164. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.6]. Supra [7.5].

[1.7] display a mobile advertisement inside the mobile software application;

1165. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.7]. Supra [7.6], [11].

[1.8] an online data publishing web service, the online data publishing web service comprising:

1166. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.8]. Hiroishi-Kahn-Bluetooth teaches about uploading (publishing) media content (data) on online service provider (online data publishing web service). The Hiroishi-Kahn-Bluetooth combination renders [1.8] obvious. In the combination, Kahn teaches an online data (image) publishing web service. Kahn teaches an image management server 330 being "a Web-based server accessible via the Internet. Kahn, [0056]. *See, e.g.*, [0056]. Kahn describes organizing images into an online photo album that may "be accessed by the user (and shared with other users) using Web browser software (e.g., Microsoft Internet Explorer)." *Id*., [0065]; *see also* FIG. 6 (showing photos being available for viewing online).

[1.9] said remote server configured with a network internet connection to communicate with the mobile software application;

1167. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.9]. Hiroishi-Kahn-Bluetooth teaches remote server configured with a network internet connection to communicate with the mobile software application. In the combination, Hiroishi teaches that the program on the mobile phone can communicate one or more remote terminals by a cellular data network and the Internet. *See, e.g.*, Hiroishi, [0048]-[0049], [0110]. For example, Hiroishi teaches that the terminals 20, 22, and 24 are configured with a network internet connection to communicate with the mobile software application. In Hiroishi, "Internet 12 is connected via a **connection device 80**, such as a modem, a router, or a TA (Terminal Adapter) to a terminal unit 20 owned by a DPE (Developing Printing Enlarging) store (hereinafter referred to as "a print shop") in various places, a terminal unit 22 installed in the house of the user of the photographing system 10, and a terminal unit 24 installed in the house of the user's friend. Mutual access of the terminal unit 20, the terminal unit 22, the terminal unit 24, and the mobile phone 40 on such a network is possible according to a predetermined communication protocol, such as TCP/IP (Transmission Control Protocol/Internet Protocol), or the like." *See, e.g.*, Hiroishi, [0049] (emphasis added).

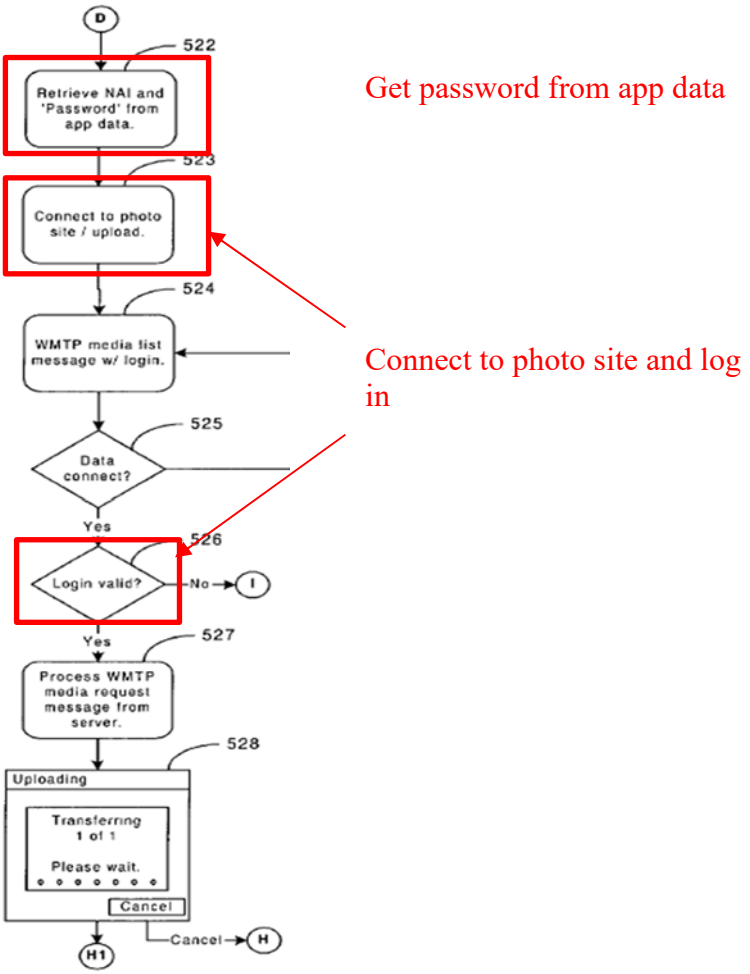
1168. To the extent that Hiroishi is shown to not teach elements of [1.9], a POSITA would have found it obvious that the remote servers were configured with an internet connection to communicate with the mobile software application, like

the servers taught by Kahn. According to Kahn, "the host device 320 communicates with an online Web-based image management server 330. In the currently preferred embodiment, the image management server 330 is a Web-based server accessible via the Internet." Kahn, [0056]. "In order to communicate with the image management server 330, the host device 320 establishes an Internet connection to the server, for example, using HTTP protocol." *Id*. A POSITA would have found it obvious that the mobile software application of Hiroishi (the program on the cellular phone) would communicate with the remote terminals using an Internet connection, like that taught by Kahn.

[1.10] a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application;

1169. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.10]. Hiroishi-Kahn-Bluetooth teaches a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application. The Hiroishi-Kahn-Bluetooth combination renders [1.10] obvious. In the combination, Kahn teaches a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application. For example, Kahn teaches "the applet retrieves the network access identifier or NAI (e.g., user cell phone number) and password." Kahn,

[0071]. The password is stored in application data, on the mobile phone, and is used as a credential for accessing the photo site for uploading. *See, e.g.*, *id*., FIG. 5C. FIG. 5C is shown below:



Kahn, FIG. 5C (partial, annotated).

1170. A POSITA would have recognized that to authenticate the user using a password, Kahn would have inherently included a software module for authenticating the user at the remote server or at a remote location connected with the server. This way, the user could "login" to the remote server, as shown by

FIG. 5C.

1171. Kahn also teaches a database that includes a database table that 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)." Kahn, [0098].

[1.11] a database, wherein the database stores a user profile; and

1172. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.11]. In the combination, Kahn teaches a database, wherein the database stores a user profile. For example, Kahn teaches a metadata database. *See, e.g.*, Kahn, [0098]. According to Kahn, the images are stored as individual files (e.g., using UNIX file system)." Kahn, [0098]. 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)." *Id*. That the database is keyed for user ID means that the database stores user profile. The user profile includes location ID. *Id*.

[1.12] a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application;

1173. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.12]. Hiroishi-Kahn-Bluetooth teaches a mobile software application advertising

software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application. For example, Kahn discloses "[d]etermination of applicable promotions …[involves] the user's location is matched against a list or database of promotions that are relevant to that user location. The resulting Set of promotions is transmitted back to the host device [mobile device], for viewing/Selection by the user" Kahn, [0087]. In FIG. 5A, Kahn illustrates that an advertisement can appear on "a client-side embedded applet (i.e., a small footprint application)" such that "the applet proceeds to display an advertisement UI dialog 510." Kahn, FIG. 5A, [0071].

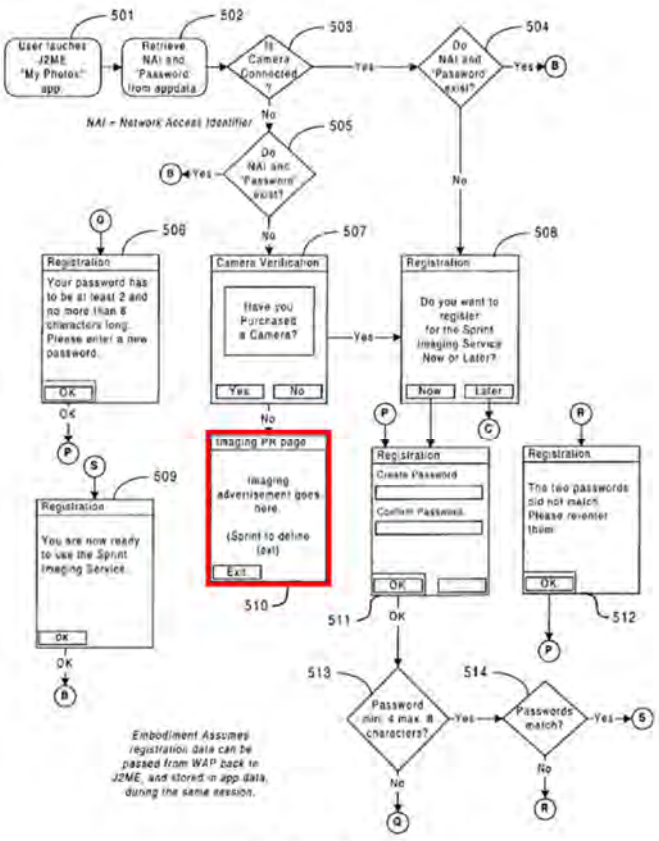


FIG. 5A

Kahn, FIG. 5A (annotated).

1174. In addition, according to Kahn, "the location information may be used to offer location-dependent promotions to the user. This may use the location information of individual photos (e.g., 20 percent off photofinishing for pictures taken at Disneyland), or may use the location information of where the user is currently located (e.g., 10 percent off photofinishing at Los Angeles-area Walgreens)." *See, e.g.*, Kahn, [0051].

1175. According to Kahn, the determination of applicable promotions operates by matching the user's location "against a list or database of promotions

that are relevant to that user location. The resulting set of promotions is transmitted back to the host device, for viewing/selection by the user, for example as a WAP page, an SMS message, an e-mail alert, or the like." Kahn, [0087]. A POSITA would have recognized the database and the software for searching and retrieving information from the database to be an advertising software module, as claimed.

[1.13] said online data publishing web service configured to receive the new-data and the user authentication credential from the Bluetooth enabled cellular phone via the Hypertext Transfer Protocol; and

1176. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.13]. Hiroishi-Kahn-Bluetooth teaches online data publishing web service configured to receive the new-data and the user authentication credential from the Bluetooth enabled cellular phone via the Hypertext Transfer Protocol. Supra [7.5.1].

[1.14] said online data publishing web service configured to process the received user authentication credential and the new-data.

1177. The Hiroishi-Kahn-Bluetooth combination renders obvious [1.14]. Hiroishi-Kahn-Bluetooth teaches online data publishing web service configured to process the received user authentication credential and the new-data. Supra [7.3].

[2] The system of claim 1, wherein the user authentication credential is stored in the memory of the Bluetooth enabled cellular phone, and wherein the user authentication credential is used by the remote server to authenticate a user.

1178. The Hiroishi-Kahn-Bluetooth combination renders obvious [2]. Supra [8].

[3] The system of claim 1, wherein the remote server is further configured to store the new-data.

1179. The Hiroishi-Kahn-Bluetooth combination renders obvious [3]. Supra [9].

[4] The system of claim 1, wherein the mobile software application provides a touch based GUI for the received new-data.

1180. The Hiroishi-Kahn-Bluetooth combination renders obvious [4]. Supra [10].

[5] The system of claim 1, wherein the mobile software application provides a touch based advertisement targeted to a user.

1181. The Hiroishi-Kahn-Bluetooth combination renders obvious [5]. Supra [11].

[6] The system of claim 1, wherein the mobile advertisement is based on the user profile.

1182. The Hiroishi-Kahn-Bluetooth combination teaches that the mobile advertisement is based on the user profile. *See supra* [1.12]. In the combination, Kahn teaches that the image manager stores the images in an image server and "stores the location ID information in the metadata database." Kahn, [0098]. "The metadata, including the location ID, is stored as a database record in a database table in the metadata database." *Id*. The database table "includes fields for user ID, timestamp (date/time), and location ID (longitude and latitude decimal values)." This database table that includes the user ID, timestamp, and location ID is a user profile. Supra [1.11]. Kahn also teaches that "the location information

may be used to offer location-dependent promotions to the user." *Id*., [0051]. Because the location information is stored in the user profile, a POSITA would have recognized Kahn for teaching that the location-dependent promotions are based on the user profile.

[12.P] A mobile software application for a Bluetooth enabled cellular phone comprising executable program instructions that, when executed by the processor controls the processor to:

1183. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.P]. Supra [7.P].

[12.1]-[12.2.2] detect and receive new-data acquired in a Bluetooth enabled data capture device, wherein the new-data is data acquired by the Bluetooth enabled data capture device after establishing a paired Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone, wherein establishing the Bluetooth paired connection comprises the Bluetooth enabled data capture device cryptographically authenticating an identity of the Bluetooth enabled cellular phone,

1184. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.1]. Supra [7.1].

[12.3.1] wherein detecting and receiving new-data acquired in the Bluetooth enabled data capture device comprises: said mobile software application for the Bluetooth enabled cellular phone configured to poll the Bluetooth enabled data capture device for new-data, over the established paired Bluetooth connection,

1185. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.2]. For example, Hiroishi discloses that the thumbnail transmission instruction is transmitted to the data capture device in step 228 of FIG. 6 and that "Thumbnails are event notifications" and polling or request for new data as shown in FIG. 7(C).

Hiroishi discloses that "[i]n the following Step 230, [the phone] waits until it receives the image data that can display the thumbnail from the digital camera 50.", TTI-1011, [0104], FIG. 7(C). A POSITA would understand that the thumbnail transmission instruction is "sending a request to the Bluetooth enabled data capture device to check if the acquired new-data is available for transfer" as part of the polling process.

The Hiroishi-Kahn-Bluetooth combination renders obvious Element [12.2]. For example, Hiroishi teaches sending, from the program running on the mobile phone, a thumbnail instruction to the camera, which is a polling instruction. *See, e.g.*, Hiroishi, [0081], [0084], [0102], FIGS. 5-6. The thumbnail instruction is sent to determine the images available in the camera's memory for transmission. *Id*. In response, the camera sends thumbnails of the images stored in camera's memory. *Id*., [0081]-[0084]. These thumbnails represent the full resolution images that are available for transfer. Supra, [7.3.1]-[7.3.2].

1186. I also note 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, a slave is only allowed to transmit **when addressed** by the LT_ADDR in the packet header in the preceding master-to-slave slot." *Id*. (emphasis added). A POSITA would have recognized that the Bluetooth operations taught by Hiroishi satisfy elements [1.3.1]-[1.3.2]. The Bluetooth Core

Specification teaches the master device polling the slave device periodically for transmissions; and the slave device only sending transmissions when it receives a LT_ADDR with the slave device addressed. *See, e.g.*, TTI-1019, 332.

[12.3.2] wherein polling comprises sending a request to the Bluetooth enabled data capture device to check if the acquired new-data is available for transfer; and;

1187. The Hiroishi-Kahn-Bluetooth combination teaches that the program on the mobile phone sends a thumbnail instruction to the camera. Supra [7.3.1]-[7.3.2], [12.3.1]. The camera response to a thumbnail instruction with a set of newly captured images stored in memory that are available for transfer. *Id*.; see also Hiroishi, [0081]-[0084], FIG. 7C. Thus, the thumbnail instruction of Hiroishi constitutes polling.

1188. In addition, or in the alternative, Hiroishi's use of Bluetooth satisfies [12.3.2]. Supra, [12.3.1]. Bluetooth uses polling to, e.g., control slave transmissions to avoid collisions on the transport channel. TTI-1019, 332 (8.6.1 Polling in the active mode).

[12.3.3] said mobile software application for the Bluetooth enabled cellular phone configured to receive, from the Bluetooth enabled data capture device, the acquired new-data over the established paired Bluetooth connection;

1189. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.3.3]. Supra [7.3.3].

[12.4] store the received new-data in a memory of the Bluetooth enabled cellular phone;

1190. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.4].

Supra [7.4].

[12.5.1]-[12.5.2] 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

1191. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.5.1]-[12.4.2]. Supra [7.5.1]-[7.5.2].

[12.6] display a mobile advertisement inside the mobile software application.

1192. The Hiroishi-Kahn-Bluetooth combination renders obvious [12.6].

Supra [7.6], [11].

[13] The mobile software application of claim 12, wherein the user authentication credential is stored in the memory of the Bluetooth enabled cellular phone, and wherein the user authentication credential is used by the remote server to authenticate a user.

1193. The Hiroishi-Kahn-Bluetooth combination renders obvious [13].

Supra [8].

[14] The mobile software application of claim 12, wherein the remote server is configured to store the new-data.

1194. The Hiroishi-Kahn-Bluetooth combination renders obvious [14].

Supra [9].

[15] The mobile software application of claim 12, wherein the mobile software application provides a touch based GUI for the received new-data.

1195. The Hiroishi-Kahn-Bluetooth combination renders obvious [15].

Supra [10].

[16] The mobile software application of claim 12, wherein the mobile software application provides a touch based advertisement targeted to a user.

1196. The Hiroishi-Kahn-Bluetooth combination renders obvious [16]. Supra [11].

B. Ground 2: Singh129 renders claims 1-16 obvious

1197. Singh129 provides the same disclosure as the '381 patent, including the subject matter disclosed in Singh906 that is incorporated by reference. *Compare* '381 patent *with* Singh129 Singh906 provides the same disclosure as the incorporated '802 application. It would have been obvious to combine Singh129 with teachings found in Singh906 to arrive at the Challenged Claims. The disclosure demonstrates that it would have been obvious in view of Singh906 to modify Singh129's: (1) database 401d to include user profiles; (2) back end service 401b to include an advertisement selection tool and an advertisement splicer; (3) client application 203 to include an advertising module that displays advertisements; and (4) new-data viewing on the mobile device's GUI.

1198. A person of ordinary skill in the art would have been motivated to make these modifications because they would have enabled Singh129's system to display targeted advertisements on mobile devices and websites (*e.g.*, "Flickr™, Picasa™, YouTube™, eBay®, etc."). Singh129, [0042]. The addition of targeted

advertising to Singh129's system would have been beneficial for various reasons. For example, it would have generated a source of revenue to support Singh129's media publishing service and thus also allow the operator of the system to make money while providing services to users at either no cost or a reduced cost. Singh906, [0008]-[0009]. The addition of targeted advertising also would have provided an incentive for advertisers to pay more for each advertisement viewed and/or have confidence that they would not pay to display advertisements to users that are not likely to be potential customers. *Id*. And the addition of targeted advertising would have given "advertisers the option to pay for each viewing of the advertisement instead of a fixed rate of payment." *Id*. (disclosing that the "publishing service utilizes the viewing information to generate advertising statistics"). Accordingly, advertisers who wished to pay only for each viewing of their advertisements would have been incentivized to pay for the display of advertisements on the proposed system rather than on competing fixed-rate systems.

1199. A person of ordinary skill in the art also would have been motivated to modify Singh129's user preferences to include authentication credentials and global positioning system information as taught by Signh906. Indeed, adding authentication credentials and global position system information to Singh129's user preferences would have given the user more control over the publishing of

their multimedia content. Singh906, [0023]. It also would have allowed the mobile device to automatically upload media to web services that required user authentication. *Id*. Furthermore, there was a known problem of associating multimedia objects with user preferences in the art as shown in Singh129, [0011]. Singh906's user preferences address that issue. And combining the teachings of Singh129 and Singh906 was not beyond the level of ordinary skill in the art. Indeed, Singh129 and Singh906 address the same problem of associating multimedia objects with user preferences. TTI-1009, [0011], [0028], [0029], [0035]-[0038], [0040, [0042], TTI-1010, Abstract, [0006], [0007]. And Singh906's user preferences, which included authentication credentials and global positioning information, were a known way to address that problem.

1200. A POSITA would have had a reasonable expectation of success when combining Singh129's disclosures as described above. Indeed, the proposed combination required no more than the application of known techniques (using an advertisement selection tool, advertisement splicer, advertising module, authentication credentials, and GPS information) to a known system (Singh129's system) in the same field of endeavor (media publishing) and from the same assignee (CellSpinSoft) to obtain the benefits described above. Furthermore, in the combination, each element merely performs the same predictable function as it does separately, without significantly hindering the functions performed by

Singh129's system. Accordingly, Singh129's system would have continued to perform all the functions it performed before the proposed modifications, including associating multimedia content with user preferences. And Singh906's advertisement selection tool, advertisement splicer, and advertising module would have continued to provide targeted advertisements on mobile devices and websites.

[1.P] A system, comprising:

1201. To the extent the preamble is limiting, the Singh129 combination renders obvious element 1.P. For example, the Singh129 combination includes a system comprising Singh129's digital data capture device 201, BT enabled mobile device 202, and publishing service 401. TTI-1009TTI-1009 (Singh129), Figs. 2, 4.

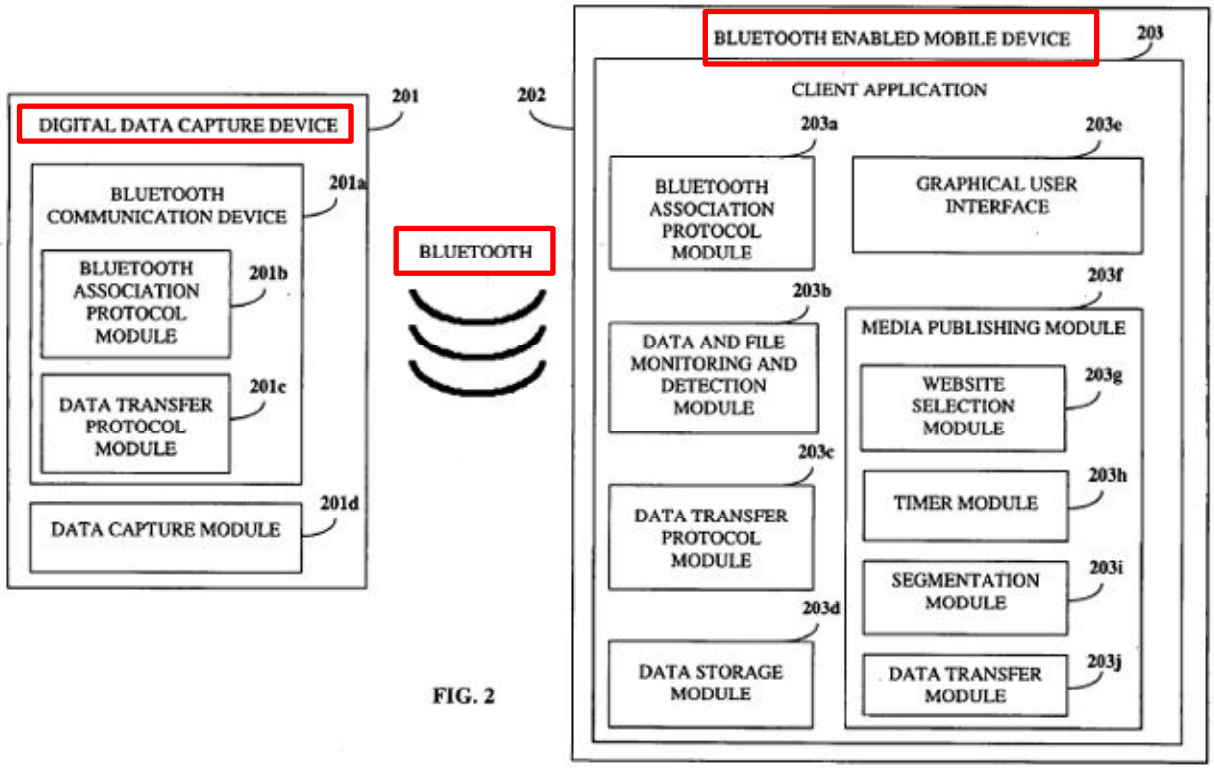
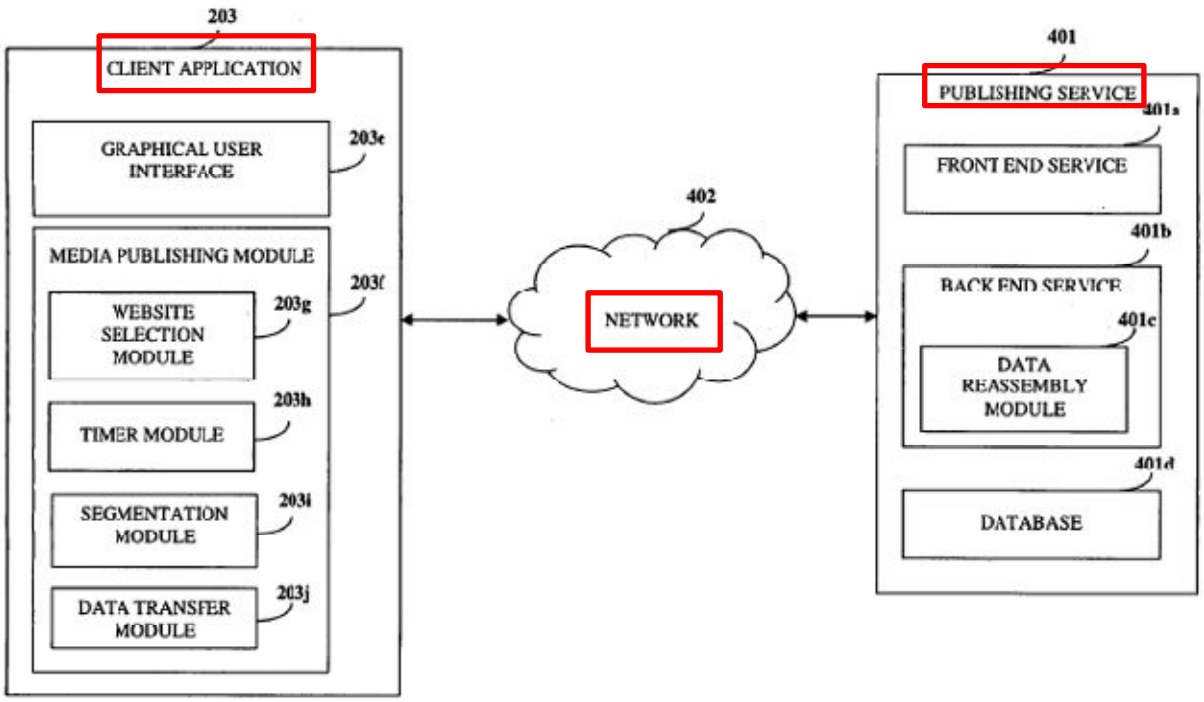


FIG. 2

Id., Fig. 2.



Id., Fig. 4.

[1.1] a mobile software application for a Bluetooth enabled cellular phone, wherein the mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, configured to:

1202. The Sing129 combination renders obvious element 1.1. The Singh129 combination includes a mobile software application (Singh129's client application 203 modified to include an advertising module as taught by Singh906) for a Bluetooth enabled cellular phone (Singh129's mobile device 202, which can be a "mobile phone"), wherein the mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, is configured to perform the recited functions as explained below. TTI-1009TTI-1009 (Singh129), Figs. 2, 4, [0020], [0046],

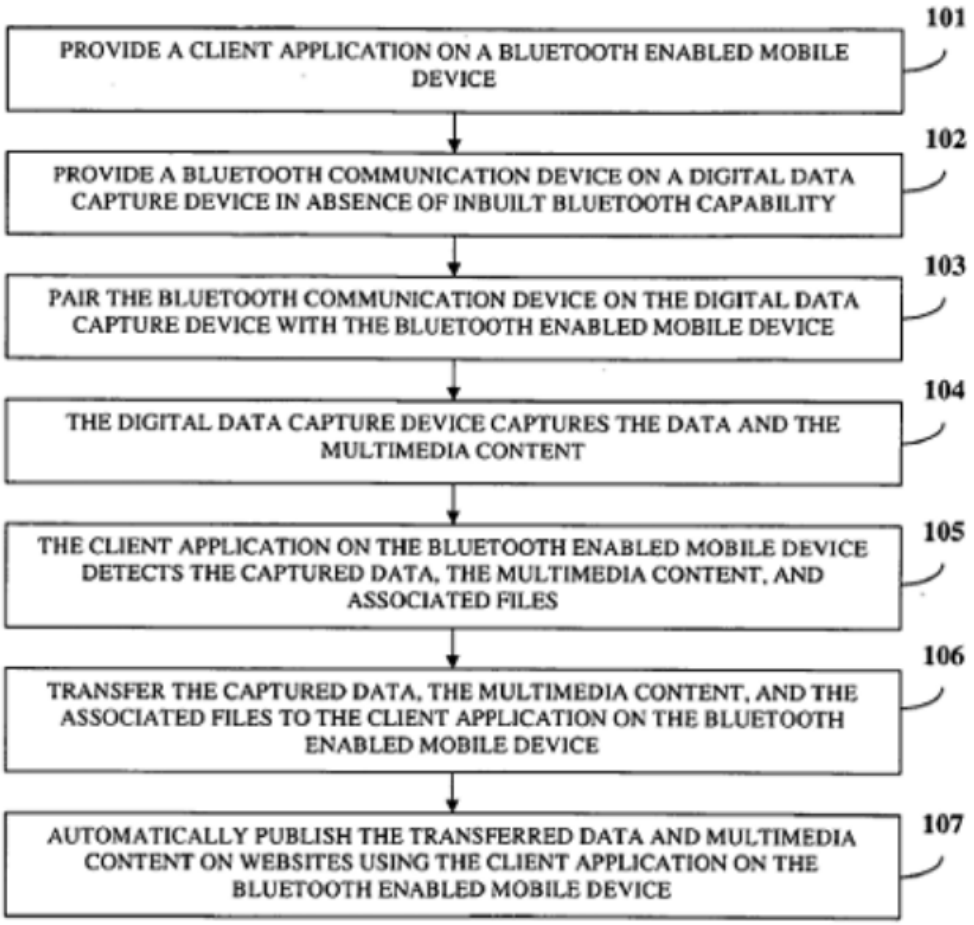
[0048] (“It will be readily apparent that the various methods and algorithms described herein may be implemented in a computer readable medium appropriately programmed for general purpose computers and computing devices. Typically, a processor … will receive instructions from a memory or like device, and execute those instructions, thereby performing one or more processes defined by those instructions.”), [0048] (“A computer program product comprising computer executable instructions embodied in a computer-readable medium comprises computer parsable codes for the implementation of the processes of various embodiments.”).

[1.2] detect and receive new-data acquired in a Bluetooth enabled data capture device,

1203. The Singh129 combination renders obvious element 1.2. The Singh129 combination’s mobile software application is configured to detect (via Singh129’s data and file monitoring and detection module 203b) and receive (via Sing129’s data transfer protocol module 203c) new-data (“the captured data, the multimedia content, and files associated with the captured data and the multimedia content”) acquired in a Bluetooth enabled data capture device (Singh129’s “Bluetooth™ enabled mobile device 202”). TTI-1009, Abstract, Figs. 1-2, [0009]-[0010], [0019], [0023], [0033]-[0034]. “The data and multimedia content may, for example, comprise image files, audio files, video files, text files, or any combination thereof.” TTI-1009, [0023].

[1.3.1] wherein the new-data is data acquired by the Bluetooth enabled data capture device after establishing a paired Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone,

1204. The Singh129 combination renders obvious element 1.3. The Singh129 combination renders obvious element 1.3.1. As shown in Figure 1 of Sing129, the new-data is data acquired by the Bluetooth enabled data capture device in step 104 after establishing (in step 103) a paired Bluetooth connection between the data capture device and the cellular phone. TTI-1009, Fig. 1, [0021]-[0023], [0033], [0041].



TTI-1009, Fig. 1.

[1.3.2] wherein establishing the Bluetooth paired connection comprises the Bluetooth enabled data capture device cryptographically authenticating an identity of the Bluetooth enabled cellular phone,

1205. The Singh129 combination renders obvious element 1.3.2. As explained in Singh129 (at [0021]), the Bluetooth paired connection (Singh129's step 103) comprises the Bluetooth enabled data capture device cryptographically authenticating an identity of the Bluetooth enabled cellular phone using "a common password known as a passkey [that] is exchanged between the BT communication device 201a and the mobile device 202." TTI-1009, [0021] ("A BT device that wants to communicate only with a trusted device can cryptographically authenticate the identity of another BT device.")

[1.4.1] wherein detecting and receiving new-data acquired in the Bluetooth enabled data capture device comprises: said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection,

1206. The Singh combination renders obvious element 1.4.1. Detecting and receiving new-data in the Bluetooth enabled data capture device comprises: said mobile software application for the Bluetooth enabled cellular phone configured to listen (via Singh129's "file event listener in the client application 203") for an event notification (Singh129's "signal from the digital data capture device 201"), sent from the Bluetooth enabled data capture device "in the event a new file is

created," over the established paired Bluetooth connection. TTI-1009, [0025]; *see also* [0021]-[0022].

[1.4.2] wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone; and

1207. The Singh129 combination renders obvious element 1.4.2. The event notification corresponds to the acquired new-data (because it is sent "in the event a new file is created") and comprises sending a signal from the Bluetooth enabled data capture device (Singh129's "signal [that is sent] from the digital data capture device 201") to the Bluetooth enabled cellular phone. TTI-1009, [0025].

[1.4.3] said mobile software application for the Bluetooth enabled cellular phone configured to receive, from the Bluetooth enabled data capture device, the event notification and the acquired new-data over the established paired Bluetooth connection;

1208. The Singh129 combination renders obvious element 1.4.3. The mobile software application for the Bluetooth enabled cellular phone is configured to receive, from the Bluetooth enabled data capture device, the event notification and the acquired new-data over the established paired Bluetooth connection. TTI-1009, [0025] ("A file event listener in the client application 203 listens for the signal from the digital data capture device 201. The user may then initiate the transfer by a press of a button or a key on the digital data capture device 201.").

[1.5] store the received new-data in a memory of the Bluetooth enabled cellular phone;

1209. The Singh129 combination renders obvious element 1.5. The mobile

software application is configured to store the received new-data in a memory (Singh129's "data storage module 203d") of the Bluetooth enabled cellular phone. TTI-1009, Fig. 2, [0033], [0035] ("The data storage module 203d stores the captured data, the multimedia content, and the associated files on the mobile device 202."), [0037] ("In the case of a mobile device 202 with limited memory and processing capabilities, the client application 203 partitions the multimedia content of large files stored on the mobile device 202 into multiple data segments using the segmentation module 203i."), [0048] (describing various forms of memory).

[1.6.1] 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,

1210. The Singh129 combination renders obvious element 1.6.1. The mobile software application is configured to use HTTP to transfer (using Singh129's data transfer module 203i) the received new-data along with a user authentication credential (Singh129's user preferences modified to include Singh906's "authentication ID", TTI-1010, [0023]) to a remote server (Singh129's front end service 401a alone or in combination with Singh129's database 401d) over a cellular data network (Singh129's network 402, which may be "a cellular network"). TTI-1009, [0039] ("The data transfer module 203i transfers the data, the tagged data segments, and the multimedia content from the client application

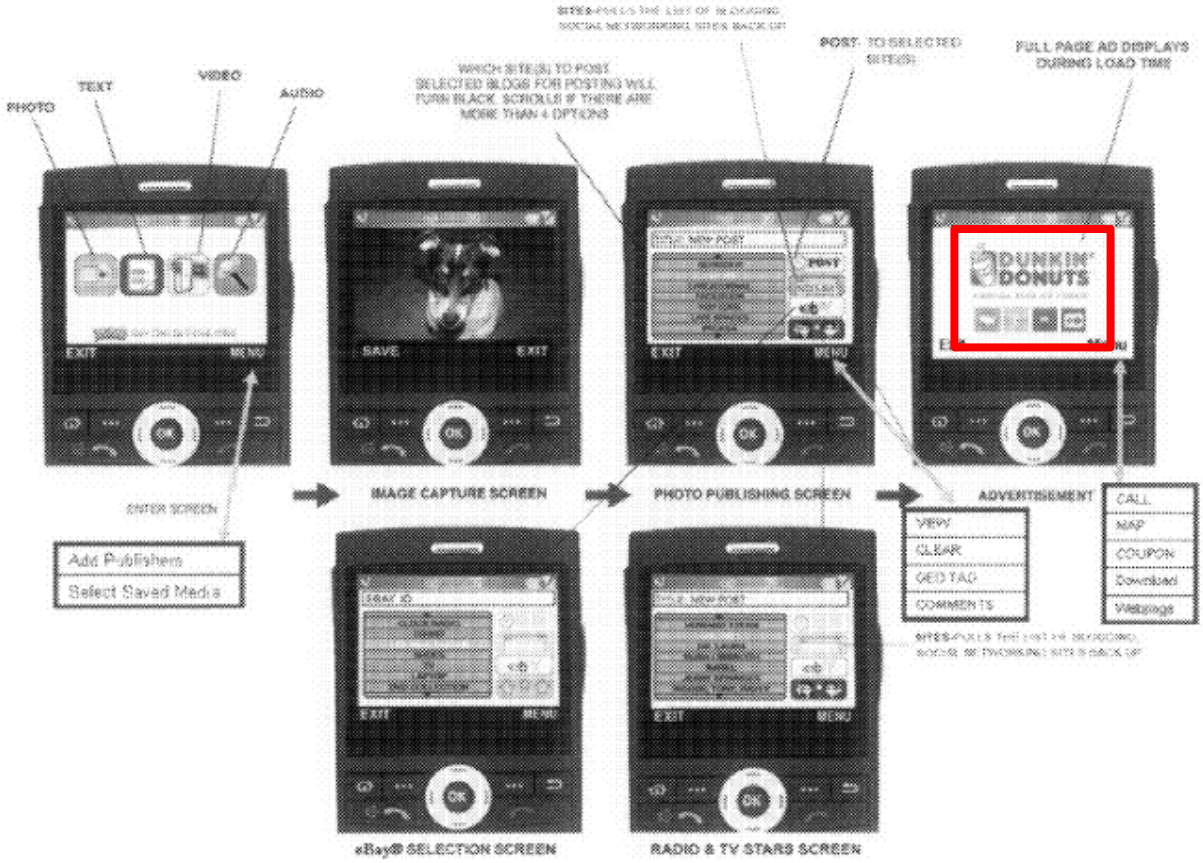
203 to the publishing service 401 via the network 402. The network 402 may, for example, be a wireless network, a cellular network, or the internet 501."), [0040] ("The data transfer module 203j [of the client application] may transfer the data and multimedia content … to the back end service 401b of the publishing service 401 via the front end service 401a."), [0047] ("The transport protocol that is used between the client application 203 and the publishing service 401 may be hypertext transfer protocol (HTTP)…."); TTI-1010, Fig. 4, [0023] ("The user preferences may comprise authentication credentials….")

[1.6.2] 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

1211. The Singh129 combination renders obvious element 1.6.2. The mobile software application is further configured to use HTTP to send a user preference (e.g., "websites selected for publishing the data and multimedia content" as taught by Singh129, authentication credentials as taught by Singh906, and/or GPS information as taught by Singh906) to the remote server over the cellular data network. TTI-1009, [0028] ("The user preferences may, for example, comprise the websites selected for publishing the data and the multimedia content."); TTI-1010, [0023] ("The user preferences may comprise authentication credentials … [and] global positioning system geographical codes….").

[1.7] display a mobile advertisement inside the mobile software application;

1212. The Singh 129 combination renders obvious element 1.7. The mobile software application is configured to display (using an advertising module 202c as taught by Singh 906) a mobile advertisement (see example below in Fig. 3 of Singh906). TTI-1010, Fig. 3, [0007], [0022] (similar), [0032] (similar). As explained in Singh906, "advertisements may…be displayed to the user 201 on the mobile device after the user 201 has published the user created multimedia content by pressing the post button on the mobile device. The advertising module 202c of the client application 202 displays advertisements targeted to the user 201 on the mobile device." *Id*., [0032]. In the combination, those advertisements would be displayed on Singh129's mobile device.



TTI-1010, Fig. 3.

[1.8] an online data publishing web service, the online data publishing web service comprising:

1213. The Singh129 combination renders obvious element 1.8. The Singh129 combination's system include an online data publishing web service (Singh129's publishing service 401 modified to include targeted advertising functionality as taught by Singh906). TTI-1009, Fig. 4, [0026];TTI-1010, Fig. 2, [0018], [0034]-[0037]; *see* Ground 1, element 1.7.

[1.9.1] said remote server configured with a network internet connection to communicate with the mobile software application;

1214. The Singh129 combination renders obvious element 1.9. The remote

server (Singh129's front end service 401a) is configured with a network connection (Singh129's network 402, which connects the client application and the publishing service) to communicate with the mobile software application. TTI-1009, Fig. 4 [0026] ("The tagged data segments are transferred from the client application 203 of the mobile device 202 to a publishing service 401 via a network 402 as illustrated in FIG. 4."), [0037]-[0039] (similar).

[1.10] a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application;

1215. The Singh129 combination renders obvious element 1.10. The online data publishing web service (element [1.8]) includes a user authentication software module (Singh906's user authentication module 204g, which is included in Singh129's publishing service in the Singh129 combination), wherein the user authentication software module processes the user authentication credential received from the mobile software application and stored in the back end service as taught by Singh906. TTI-1010, Abstract ("A protocol is provided for synchronizing user preferences of the publication virtual spaces between the client application and the publishing service."), Fig. 1 (Step 104), Fig. 4 (steps 407, 410), [0028] ("The preferences set by the user [in the mobile software application] may be authentication credentials…."), [0034] ("The publishing service 204 comprises … a user authentication module 204g."), [0035] ("The back end service 204c is

provided with credentials for user authentication…. The user authentication module 204g authenticates the user 201 of the client application 202."), [0037] ("The user 201 is authenticated before publishing the user created multimedia content…."), [0047] ("Additional information such … authentication identification … are selected 407 and transferred along with the user created multimedia content to the publishing service 204.), [0049] ("The front end service 204b … authenticates 410 the user 201….").

[1.11] a database, wherein the database stores a user profile; and

1216. The Singh129 combination renders obvious element 1.11. The online data publishing web service (element [1.8]) includes Singh129's database 401d, which is modified to store a user profile as taught by Singh906. TTI-1009, Fig. 4, [0040], [0049]; TTI-1010, Fig. 2, [0034] ("The database 204a of the publishing service 204 comprises user profiles….").

[1.12] a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application;

1217. The Singh129 combination renders obvious element 1.12. The online data publishing web service (element [1.8]) includes a mobile software application advertising software module (Singh906's backend service 204c, which includes advertisement selection tool 204e), wherein the mobile software application advertising software module selects advertisements based on the user profile and

sends the selected advertisements (via Singh129's front end service 401a and network 402) to the mobile software application. TTI-1010, Figs. 2-3, [0032] ("Optional advertisements may also be displayed to the user 201 on the mobile device after the user 201 has published the user created multimedia content by pressing the post button on the mobile device. The advertising module 202c of the client application 202 displays advertisements targeted to the user 201 on the mobile device."), [0036] ("Targeted advertisements based on the user profile may be selected from the database 204a of the publishing service 204 by the advertisement selection tool 204e. The advertisement selection tool 204e of the back end service 204c selects advertisements from the database 204a based on the user profile 201….").

[1.13] said online data publishing web service configured to receive the new-data and the user authentication credential from the Bluetooth enabled cellular phone via the Hypertext Transfer Protocol; and

1218. The Singh129 combination renders obvious element [1.13]. The online data publishing web service (element [1.8]) is configured to receive the new-data and the user authentication credential from the Bluetooth enabled cellular phone via HTTP. *See* Ground 1, element [1.6.1].

[1.14] said online data publishing web service configured to process the received user authentication credential and the new-data.

1219. The Singh129 combination renders obvious element 1.14. The online data publishing web service (element [1.8]) is configured to process the received

user authentication credential (e.g., using the authentication credential to authenticate the user) and the new-data (e.g., reassembling the data segments, splicing advertisement into the new data, and/or publishing the new-data with advertisements). Ground 1, element [1.10] (processing the received user authentication credential); TTI-1009, [0040] ("If the back end service 401b receives the multimedia content in the form of multiple data segments, the data reassembly module 401c reassembles the data segments in a predetermined sequence using the segment identifiers."), TTI-1010, [0024] ("The back end service 204c may then splice the multimedia object with targeted advertisements based on the user profile. The multimedia object is then transferred 107 from the back end service 204c to the front end service 204b and published 108 by the front end service 204b on one or more publication virtual spaces 205 according to user preferences.").

2. The system of claim 1, wherein the user authentication credential is stored in the memory of the Bluetooth enabled cellular phone, and wherein the user authentication credential is used by the remote server to authenticate a user.

1220. The Singh129 combination renders obvious claim 2. The user authentication credential (*see* [1.5]) is stored in the memory of the Bluetooth enabled cellular phone. TTI-1009, Fig. 2, [0042]; TTI-1010, [0028], ("The client application 202 may have default settings, but the user 201 may also set preferences on the mobile device. The preferences set by the user 201 may be

authentication credentials". In the combination, Singh129's user preferences include user authentication credentials. And Singh129 confirms that the "user 502 may … store the preferences on the mobile device 202." TTI-1009, [0042]. As explained in Ground 1, elements [1.10] and [1.14], the user authentication credential is used by the remote server to authenticate a user.

3. The system of claim 1, wherein the remote server is further configured to store the new-data.

1221. The Singh129 combination renders obvious claim 3. The remote server (*see* [1.6.1]) is configured to store the new-data. TTI-1009, [0040] ("The transferred data and multimedia content is stored in the database 401d of the publishing service 401.").

4. The system of claim 1, wherein the mobile software application provides a touch based GUI for the received new-data.

1222. The Singh129 combination renders obvious claim 4. The mobile software application (*see* [1.1]-[1.7]) provides a touch based GUI (Singh129's GUI 203e) for the received new-data. TTI-1009, [0033] ("The client application 203 on the mobile device 202 comprises … a graphical user interface (GUI) 203e…."). "The user may also set preferences on the mobile device 202 using the GUI 203e of the client application 203. The user preferences may, for example, comprise the websites selected for publishing the data and the multimedia content. The GUI 203e enables the user to configure a timer setting and websites on the mobile

device 202 for publishing the data and the multimedia content. The user may also set timer and action settings for publishing the data and the multimedia content using the GUI 203e." TTI-1009, [0035]. In the Singh combination, the new-data can be viewed on the GUI, "The user 201 may also review the recording", Ex-1010, [0030]."

5. The system of claim 1, wherein the mobile software application provides a touch based advertisement targeted to a user.

1223. The Singh129 combination renders obvious claim 5. As explained in Ground 1, element [1.7], the mobile software application provides an advertisement to the user on the touch screen of the mobile device. That advertisement is a touch based advertisement. TTI-1010, Fig. 3, [0023] ("Depending on the interface provided by the mobile device, the single input action of the user 201 may be a click or touch of a button provided on the graphical user interface 202a of the mobile device….").

6. The system of claim 1, wherein the mobile advertisement is based on the user profile.

1224. The Singh129 combination renders obvious claim 6. As explained in Ground 1, element [1.12], the mobile advertisement is based on the user profile.

Claim 7

1225. *See* Claim 1, elements [1.1]-[1.7].

Claims 8-11

1226. *See* Claims 2-5.

Claim 12

[12.P-12.2.2], [12.3.3-12.6]

1227. *See* Ground 2, [1.1]-[1.3.2], [1.4.3]-[1.8].

[12.3.1]-[12.3.2] wherein detecting and receiving new-data acquired in the Bluetooth enabled data capture device comprises: said mobile software application for the Bluetooth enabled cellular phone configured to poll the Bluetooth enabled data capture device for new-data, over the established paired Bluetooth connection,

1228. The Singh129 combination renders obvious element [12.3.1-[12.3.2]. Detecting and receiving new-data in the Bluetooth enabled data capture device comprises: said mobile software application for the Bluetooth enabled cellular phone configured to (in the "pull mode") poll the Bluetooth enabled data capture device, over the established paired Bluetooth connection. TTI-1009, [0023] ("In the pull mode, the client application 203 periodically polls the digital data capture device 201 to determine the creation of a new file in the digital data capture device 201.").

XV. CONCLUSION

I currently hold the opinions set expressed in this declaration. But my analysis may continue, and I may acquire additional information and/or attain supplemental insights that may result in added observations.

I hereby declare that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true. I further declare that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of the Title 18 of the United States Code.

Dated: 04/05/2024 By: David B. Lett

David B. Lett

XVI. APPENDIX

The claims of the Challenged Patents are shown below with a numeric mapping for ease of reference:

A. '030 CLAIMS LISTING

'030 patent	
1.P	A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:
1.1	performing at a Bluetooth enabled data capture device:
1.2	establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;
1.3	sending a message to the Bluetooth enabled mobile device, corresponding to supported data capability of the Bluetooth enabled data capture device;
1.4	[1.4.1] acquiring new data in the Bluetooth enabled data capture device, [1.4.2] wherein new data is data acquired after the paired secure Bluetooth

	connection is established;
1.5	detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises:
1.6	receiving a request to get new data, at the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired Bluetooth connection;
1.7	receiving a request to enable event notifications for new data on the Bluetooth enabled data capture device, from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection;
1.8	enabling event notification on Bluetooth enabled data capture device, corresponding to new data;
1.9	determining existence of the new data for transfer; and
1.10	sending event notification as a signal to the Bluetooth enabled mobile device, corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device listens for the event notification sent from the Bluetooth enabled data capture device;

1.11	encrypting, using cryptographic encryption key, the new data acquired in the Bluetooth enabled data capture device; and
1.12	transferring the encrypted data from the Bluetooth enabled data capture to the Bluetooth enabled mobile device, over the paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data and obtain the new data from the encrypted data using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by the remote internet server.
2	The method of claim 1, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.
3.	The method of claim 1, wherein Bluetooth capability is provided to

	the Bluetooth enabled data capture device by an external Bluetooth module.
4.	The method of claim 1, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.
5.	The method of claim 1, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.
6.P	A method for transferring data from a Bluetooth enabled data capture device to a remote internet server via a Bluetooth enabled mobile device comprising:
6.1	performing at a Bluetooth enabled data capture device:
6.2	establishing a paired secure Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device, wherein the paired secure Bluetooth connection uses cryptographic encryption key;
6.3	acquiring new data in the Bluetooth enabled data capture device, wherein new data is data acquired after the paired secure Bluetooth connection is established;

6.4	detecting and signaling the new data for transfer, to the Bluetooth enabled mobile device, wherein detecting and signaling the new data for transfer comprises:
6.5	receiving a message from the Bluetooth enabled mobile device, over the established paired secure Bluetooth connection, to register for data signal notifications, wherein the data signal notifications correspond to existence of new data for transfer on the Bluetooth enabled data capture device;
6.6	determining existence of the new data for transfer; and
6.7	creating a new data object on the Bluetooth enabled data capture device, wherein the new data object comprises new data, data associated with new data and a data signal notification, wherein data signal notification is a **time-stamp attribute** inside the data object, wherein the data signal notification corresponds to existence of new data for transfer, and wherein the time-stamp corresponds to a time when new data was acquired;
6.8	encrypting, using cryptographic encryption key, the new data object in the Bluetooth enabled data capture device; and
6.9	transferring the encrypted data object from the Bluetooth enabled data capture device to the Bluetooth enabled mobile device, over the

	established paired secure Bluetooth connection, wherein the Bluetooth enabled mobile device has access to the internet, wherein the Bluetooth enabled mobile device is configured to receive the encrypted data object and obtain the new data and the data signal notification from the encrypted data object using cryptographic encryption key, wherein the Bluetooth enabled mobile device is configured to apply action setting and destination web address of a remote internet server to the obtained new data, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, wherein the Bluetooth enabled mobile device is configured to send the obtained new data along with a user identifier to a remote internet server, wherein the user identifier uniquely identifies a particular user of internet service provided by a remote internet server.
7.	The method of claim 6, wherein Bluetooth capability is provided internally in the Bluetooth enabled data capture device.
8.	The method of claim 6, wherein Bluetooth capability is provided to the Bluetooth enabled data capture device by an external Bluetooth module.
9.	The method of claim 6, wherein the new data for transfer comprises

	one or more of audio data, video data, image data, text data, or digital data.
10.	The method of claim 6, wherein said data signal notification corresponds to creation of new data for transfer or change in status of new data for transfer.
11.	The method of claim 6, wherein the time-stamp is either absolute time or relative time.
12.P	12. A method for transferring data to a remote internet server by a Bluetooth enabled mobile device comprising:
12.1	providing a software module on the Bluetooth enabled mobile device, wherein the software module on the Bluetooth enabled mobile device is configured to perform steps comprising:
12.2	establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein paired secure Bluetooth connection uses cryptographic encryption key;
12.3	receiving a message from the Bluetooth enabled data capture device, corresponding to supported data capability of the Bluetooth enabled data capture device;

12.4	detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:
12.5.1	sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data,
12.5.2	wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;
12.6	enabling event notification listening on Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;
12.7	receiving, from the Bluetooth enabled data capture device, an event notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and
12.8	sending a request to the Bluetooth enabled data capture device, to get new data for transfer;

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

15.1	performing at a Bluetooth enabled mobile device:
15.2	establishing a paired secure connection between the Bluetooth enabled mobile device and a Bluetooth enabled data capture device, wherein the secure paired Bluetooth connection uses cryptographic encryption key;
15.3	detecting new data acquired by the Bluetooth enabled data capture device for transfer, wherein detecting the new data for transfer comprises:
15.4	sending a message to the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection, to enable event notifications on the Bluetooth enabled data capture device corresponding to new data, wherein the new data is data acquired by Bluetooth enabled data capture device after establishing the secure Bluetooth pairing connection between the Bluetooth enabled data capture device and the Bluetooth enabled mobile device;
15.5	enabling event notification listening on the Bluetooth enabled mobile device, to listen for event notifications sent from the Bluetooth enabled data capture device, over the established paired secure Bluetooth connection;
15.6	receiving, from the Bluetooth enabled data capture device, an event

	notification corresponding to existence of new data for transfer, over the established paired secure Bluetooth connection; and
15.7	sending a request to the Bluetooth enabled data capture device, to get new data object for transfer, wherein new data object comprises of new data, data associated with new data and time-stamp, and wherein the time-stamp corresponds to a time when new data was acquired;
15.8	receiving, by the Bluetooth enabled mobile device, encrypted data object corresponding to the new data object over the established Bluetooth paired wireless connection;
15.9	obtaining new data, data associated with new data and time-stamp from the received encrypted data object using cryptographic encryption key; and
15.10	sending the obtained new data and the obtained time-stamp along with a user identifier to a remote internet server, comprising configuring the obtained new data to comprise an action setting and destination web address of a remote internet server, wherein action setting comprises one of a remote procedure call (RPC) method and hypertext transfer protocol (HTTP) method, and wherein the user identifier uniquely identifies a particular user of the internet service

	provided by a remote internet server.
16.	The method of claim 15, wherein the new data for transfer comprises one or more of audio data, video data, image data, text data, or digital data.
17.	The method of claim 15, wherein event notification corresponds to creation of new data for transfer or change in status of new data for transfer.
18.	The method of claim 6, wherein the time-stamp is either absolute time or relative time.

B. '766 CLAIMS LISTING

'766 patent	
1.P	A short-range wireless enabled data capture device, comprising:
1.1	a memory device;
1.2	a processor coupled to said memory device;
1.3	a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone,
1.4	wherein establishing the short-range paired wireless connection comprises cryptographically authenticating identity of the short-range wireless enabled cellular phone, and
1.5	wherein establishing the short-range paired wireless connection further comprises the short-range wireless enabled data capture device using an association protocol;
1.6	a data capture circuitry;
1.7	said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry,
1.8	wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless

	enabled data capture device and the short-range wireless enabled cellular phone;
1.9	said processor further configured to store the new-data in the memory device;
1.10	said processor further configured to create a new-data object, wherein the new-data object comprises:
1.11	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;
1.12	the acquired new-data; and
1.13	associated new-data, wherein the associated new-data corresponds to data associated with the new-data; and
1.14	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,
1.15	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,
1.16.1	wherein a mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the signal to notify
1.16.2	and store the received new-data in a memory device of the cryptographically authenticated short-range wireless enabled cellular phone,
1.17	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
1.18	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.	The short-range wireless enabled data capture device of claim 1, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking

	technologies that use pairing.
3.	The short-range wireless enabled data capture device of claim 1, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.
4.P	A system, comprising:
4.1	a data capture device, comprising:
4.2	a first memory device;
4.3	a first processor coupled to the first memory device;
4.4	a first short-range wireless communication device configured to establish a short-range paired wireless connection with an internet connected cellular phone,
4.5	wherein establishing the short-range paired wireless connection comprises, the data capture device cryptographically authenticating identity of the cellular phone, and
4.6	wherein establishing the short-range paired wireless connection further comprises the data capture device using an association protocol;
4.7	a data capture circuitry;

4.8	said first processor configured to acquire new-data in the data capture device using the data capture circuitry,
4.9	wherein the new-data is data acquired after establishing the short-range paired wireless connection with the cellular phone;
4.10	said first processor further configured to store the new-data in the first memory device;
4.11	said first processor further configured to create a new-data object, wherein the new-data object comprises:
4.12	signal to notify, wherein the signal to notify corresponds to the acquiring of the new-data for transfer to the cryptographically authenticated cellular phone;
4.13	the acquired new-data; and
4.14	associated new-data, wherein the associated new-data corresponds to data associated with the new-data; and
4.15	said first processor further configured to transfer automatically the new-data object to the cryptographically authenticated cellular phone, over the established short-range paired wireless connection;
4.16	said cellular phone, comprising:
4.17	a second memory device;

4.18	a second processor coupled to said second memory device;
4.19	a cellular network communication device configured to connect to the internet via the cellular data network;
4.20	a second short-range wireless communication device configured to establish the short-range paired wireless connection between the cellular phone and the data capture device;
4.21	a mobile client application for the cellular phone comprising executable instructions that, when executed by the second processor controls the second processor to:
4.22	listen for the signal to notify;
4.23	receive the new-data object from the data capture device;
4.24	store the received new-data in the second memory device; and
4.25	use HTTP to transfer the new-data along with user information to a user data publishing website over the cellular data network,
4.26	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.
5.	The system of claim 4, wherein establishing the short-range paired

	wireless connection comprises the data capture device using an association protocol.
6.	The system of claim 4, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.
7.	The system of claim 4, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.
8.	The system of claim 4, wherein a graphical user interface (GUI) is provided in the cryptographically authenticated cellular phone, and wherein the graphical user interface (GUI) is for the received new-data.
9.P	A short-range wireless enabled cellular phone, comprising:
9.1	a memory device;
9.2	a processor coupled to said memory device;
9.3	a cellular network communication device configured to connect to internet via a cellular data network;
9.4	a short-range wireless communication device configured to establish

	a short-range paired wireless connection between the short-range wireless enabled cellular phone and a short-range wireless enabled data capture device,
9.5	wherein the short-range wireless enabled data capture device is configured to cryptographically authenticate identity of the short-range wireless enabled cellular phone when establishing the short-range paired wireless connection, and
9.6	wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled mobile device using an association protocol;
9.7	a mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that, when executed by the processor controls the processor to:
9.8	receive a new-data object from the short-range wireless enabled data capture device over the established short-range paired wireless connection,
9.9	wherein the new-data object comprises:
9.10	signal to notify and acquired new-data,
9.11	wherein the acquired new-data is data acquired by the short-range

	wireless enabled data capture device after the short-range paired wireless connection is established between the short-range wireless enabled cellular phone and the short-range wireless enabled data capture device, and
9.12	wherein the signal to notify corresponds to the acquiring of the new-data for transfer; and
9.13	associated new-data, wherein the associated new-data corresponds to data associated with the new-data;
9.14	listen and process the signal to notify;
9.15	store the received new-data in the memory device; and
9.16	use HTTP to transfer the new-data along with user information to a user data publishing website over the cellular data network,
9.17	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.
10.	The short-range wireless enabled cellular phone of claim 9, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and

	other wireless personal area networking technologies that use pairing.
11.	The short-range wireless enabled cellular phone of claim 9, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.
12.	The short-range wireless enabled cellular phone of claim 9, wherein a graphical user interface (GUI) is provided in the cryptographically authenticated short-range wireless enabled cellular phone, and wherein the graphical user interface (GUI) is for the received new-data.
13.P	A system, comprising:
13.1	a short-range wireless enabled data capture device, comprising:
13.2	a first memory device;
13.3	a first processor coupled to the first memory device;
13.4	a first short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone,
13.5	wherein establishing the short-range paired wireless connection

	comprises cryptographically authenticating identity of the short-range wireless enabled cellular phone, and
13.6	wherein establishing the short-range paired wireless connection further comprises the short-range wireless enabled data capture device using an association protocol;
13.7	a data capture circuitry;
13.8	said first processor configured to acquire new-data using the data capture circuitry, wherein the new-data is data acquired after the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone is established;
13.9	said first processor further configured to store the acquired new-data in the first memory device;
13.10	said processor further configured to create a new-data object, wherein the new-data object comprises:
13.11	signal to notify, wherein the signal to notify corresponds to the acquiring of the new-data for transfer;
13.12	the acquired new-data; and
13.13	associated new-data, wherein the associated new-data corresponds to

	data associated with the new-data; and
13.14	said first processor further configured to receive a data transfer request from the short-range wireless enabled cellular phone, over the established short-range paired wireless connection,
13.15	wherein the data transfer request is for the acquired new-data that was acquired by the short-range wireless enabled data capture device before receiving the data transfer request; and
13.16	said first processor configured to transfer the new-data object to the short-range wireless enabled cellular phone over the established short-range paired wireless connection;
13.17	a mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that, when executed by a second processor of the short-range wireless enabled cellular phone controls the second processor to:
13.18	receive a request through a graphical user interface (GUI) of the cryptographically authenticated short-range wireless enabled cellular phone for new-data and send a data transfer request to the short-range wireless enabled data capture device, over the established short-range paired wireless connection,
13.19	wherein the data transfer request is for the acquired new-data that

	was acquired by the short-range wireless enabled data capture device before receiving the data transfer request;
13.20	receive the new-data object from the short-range wireless enabled data capture device, over the established short-range paired wireless connection;
13.21	store the new-data received over the established short-range paired wireless connection, in a second memory device of the short-range wireless enabled cellular phone; and
13.22	use HTTP to upload the new-data along with user information to a user data publishing website over the cellular data network,
13.23	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.
14.	The system of claim 13, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.
15.	The system of claim 13, wherein the new-data comprises one or more of audio data, video data, image data, text data, digital data,

	and data associated with the new-data.

C. '121 CLAIMS LISTING

'121 patent	
1.P	A short-range wireless enabled data capture device, comprising:
1.1	a memory device;
1.2	a processor coupled to the memory device;
1.3.1	a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone,
1.3.2	wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled data capture device cryptographically authenticating identity of the short-range wireless enabled cellular phone;
1.4	a data capture circuitry;
1.5.1	said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry,
1.5.2	wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;

1.6	said processor further configured to store the new-data in the memory device;
1.7.1	said processor further configured to send an event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically,
1.7.2	wherein the event notification corresponds to the acquired new-data and comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone,
1.8	wherein the cryptographically authenticated short-range wireless enabled cellular phone is configured to listen to the event notification and receive the new-data over the established short-range paired wireless connection,
1.9.1	wherein a single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the event notification and
1.9.2	store the received new-data in a memory device of the cryptographically authenticated short-range wireless enabled cellular phone,
1.10	wherein the single mobile client application for the cryptographically

	authenticated short-range wireless enabled cellular phone stores a user authentication credential in the memory device of the cryptographically authenticated short-range wireless enabled cellular phone,
1.11	wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to use HTTP to upload the received new-data and the user authentication credential to a user data publishing website over a cellular data network,
1.12	wherein the upload is based on a timer setting on the single mobile client application, wherein the timer setting is no wait automatic or wait X minutes automatic,
1.13	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
1.14	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.

2.	The short-range wireless enabled data capture device of claim 1, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.
3.	The short-range wireless enabled data capture device of claim 1, wherein the user authentication credential sent by the single mobile client application is used to authenticate a user on the user data publishing website and publish the new-data for private use on the user data publishing website.
4.P	A system, comprising:
4.1	a short-range wireless enabled data capture device, comprising:
4.2	a first memory device;
4.3	a first processor coupled to the first memory device;
4.4.1	a first short-range wireless communication device configured to establish a short-range paired wireless connection with a short-range wireless enabled cellular phone,
4.4.2	wherein the short-range wireless enabled cellular phone is internet enabled,

4.4.3	wherein establishing the short-range paired wireless connection comprises, the short-range wireless enabled data capture device cryptographically authenticating identity of the short-range wireless enabled cellular phone;
4.5	a data capture circuitry;
4.6.1	said first processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry,
4.6.2	wherein the new-data is data acquired after establishing the short-range paired wireless connection with the short-range wireless enabled cellular phone;
4.7	said first processor further configured to store the new-data in the first memory device; and
4.8.1	said first processor further configured to send an event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically,
4.8.2	wherein the event notification corresponds to the acquired new-data and comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone;

4.9	said short-range wireless enabled cellular phone, comprising: a second memory device;
4.10	a second processor coupled to the second memory device;
4.11	a cellular network communication device configured to connect to the internet via a cellular data network;
4.12	a second short-range wireless communication device configured to establish the short-range paired wireless connection between the short-range wireless enabled cellular phone and the short-range wireless enabled data capture device;
4.13	a single mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that, when executed by the second processor controls the second processor to:
4.14.1	listen for the event notification sent by the short-range wireless enabled data capture device,
4.14.2	wherein the single mobile client application for the short-range wireless enabled cellular phone is configured to process the event notification;
4.15	receive the new-data from the short-range wireless enabled data capture device;

4.16	store the received new-data in the second memory device;
4.17	store a user authentication credential in the second memory device;
4.18.1	use HTTP to upload the received new-data and the user authentication credential to a user data publishing website over the cellular data network,
4.18.2	wherein the upload is based on a timer setting on the single mobile client application, and wherein the timer setting is no wait automatic or wait X minutes automatic;
4.19	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
4.20	provide a touch based graphical user interface for the received new-data.
5.	The system of claim 4, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.
6.	The system of claim 4, wherein the user authentication credential is for a user of the user data publishing website.

7.P	A short-range wireless enabled cellular phone, comprising:
7.1	a memory device;
7.2	a processor coupled to the memory device;
7.3	a cellular network communication device configured to connect to internet via a cellular data network;
7.4.1	a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled cellular phone and a short-range wireless enabled data capture device,
7.4.2	wherein the short-range wireless enabled data capture device is configured to cryptographically authenticate identity of the short-range wireless enabled cellular phone;
7.5	a single mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that, when executed by the processor controls the processor to:
7.6	[7.6.1] listen for an event notification sent by the short-range wireless enabled data capture device, wherein the event notification corresponds to new-data and comprises sending a signal by the short-

	range wireless enabled data capture device to the short-range wireless enabled cellular phone, [7.6.2] wherein the new-data is data acquired by the data capture device after establishing the short-range paired wireless connection with the short-range wireless enabled cellular phone;
7.7	receive the event notification and the new-data from the short-range wireless enabled data capture device;
7.8.1	process the event notification and
7.8.2	store the received new-data in the memory device;
7.9	store a user authentication credential in the memory device;
7.10	[7.10.1] use HTTP to send a user preference to a user data publishing web service over the cellular data network, [7.10.2] wherein the user preference comprises global positioning system information;
7.11	[7.11.1] further use the HTTP to upload the received new-data and the user authentication credential to the user data publishing web service over

	the cellular data, [7.11.2] wherein the upload is based on a timer setting on the single mobile client application, and wherein the timer setting is no wait automatic or wait X minutes automatic; and
7.12	provide a touch based graphical user interface for the received new-data.
8.	The short-range wireless enabled cellular phone of claim 7, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.
9.P	A short-range wireless enabled data capture device, comprising:
9.1	a memory device;
9.2	a processor coupled to the memory device;
9.3.1	a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone,

9.3.2	wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled data capture device cryptographically authenticating identity of the short-range wireless enabled cellular phone;
9.4	a data capture circuitry;
9.5.1	said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry,
9.5.2	wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;
9.6	said processor further configured to store the new-data in the memory device of the short-range wireless enabled data capture device;
9.7.1	said processor further configured to listen to a polling request from a single mobile client application on the short-range wireless enabled cellular phone, over the established paired short-range wireless connection, wherein the polling request is for the new-data,
9.7.2	wherein the single mobile client application on the short-range wireless enabled cellular phone is configured to detect the new-data

	for transfer from the short-range wireless enabled data capture device to the paired and the cryptographically authenticated short-range wireless enabled cellular phone,
9.8	wherein detecting the new-data for transfer comprises: polling the short-range wireless enabled data capture device by the short-range wireless enabled cellular phone, using the single mobile client application on the short-range wireless enabled cellular phone, over the established paired short-range wireless connection;
9.9	said processor further configured to transfer the new-data from the short-range wireless enabled data capture device to the short-range wireless enabled cellular phone automatically over the established paired short-range wireless connection,
9.10	wherein the single mobile client application on the short-range wireless enabled cellular phone is further configured to receive the new-data over the established short-range paired wireless connection,
9.11	wherein the single mobile client application on the short-range wireless enabled cellular phone is further configured to store the received new-data in a memory device of the short-range wireless enabled cellular phone,

9.12	wherein the single mobile client application for the short-range wireless enabled cellular phone stores a user authentication credential in the memory device of the short-range wireless enabled cellular phone,
9.13	wherein the single mobile client application on the short-range wireless enabled cellular phone is further configured to use HTTP to send a user preference to a user data publishing website over a cellular data network, wherein the user preference comprise global positioning system information,
9.14	wherein the single mobile client application on the short-range wireless enabled cellular phone is further configured to use the HTTP to upload the received new-data and the user authentication credential to the user data publishing website over the cellular data network,
9.15	wherein the upload is based on a timer setting on the single mobile client application, and wherein the timer setting is no wait automatic or wait X minutes automatic, and
9.16	wherein the single mobile client application on the short-range wireless enabled cellular phone provides a touch based GUI for the received new-data.

10.	The short-range wireless enabled data capture device of claim 9, wherein the short-range paired wireless connection is one of a Bluetooth paired wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

D. ’381 CLAIMS LISTING

’381 patent	
1.P	A system, comprising:
1.1	a mobile software application for a Bluetooth enabled cellular phone, wherein the mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, configured to:
1.2	detect and receive new-data acquired in a Bluetooth enabled data capture device,
1.3.1	wherein the new-data is data acquired by the Bluetooth enabled data capture device after establishing a paired Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone,
1.3.2	wherein establishing the Bluetooth paired connection comprises the Bluetooth enabled data capture device cryptographically authenticating an identity of the Bluetooth enabled cellular phone,
1.4.1	wherein detecting and receiving new-data acquired in the Bluetooth enabled data capture device comprises: said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data

	capture device, over the established paired Bluetooth connection,
1.4.2	wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone; and
1.4.3	said mobile software application for the Bluetooth enabled cellular phone configured to receive, from the Bluetooth enabled data capture device, the event notification and the acquired new-data over the established paired Bluetooth connection;
1.5	store the received new-data in a memory of the Bluetooth enabled cellular phone;
1.6.1	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,
1.6.2	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
1.7	display a mobile advertisement inside the mobile software application;

1.8	an online data publishing web service, the online data publishing web service comprising:
1.9	said remote server configured with a network internet connection to communicate with the mobile software application;
1.10	a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application;
1.11	a database, wherein the database stores a user profile; and
1.12	a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application;
1.13	said online data publishing web service configured to receive the new-data and the user authentication credential from the Bluetooth enabled cellular phone via the Hypertext Transfer Protocol; and
1.14	said online data publishing web service configured to process the received user authentication credential and the new-data.
2.	The system of claim 1, wherein the user authentication credential is stored in the memory of the Bluetooth enabled cellular phone, and

	wherein the user authentication credential is used by the remote server to authenticate a user.
3.	The system of claim 1, wherein the remote server is further configured to store the new-data.
4.	The system of claim 1, wherein the mobile software application provides a touch based GUI for the received new-data.
5.	The system of claim 1, wherein the mobile software application provides a touch based advertisement targeted to a user.
6.	The system of claim 1, wherein the mobile advertisement is based on the user profile.
7.P	A mobile software application for a Bluetooth enabled cellular phone, wherein the mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, configured to:
7.1	detect and receive new-data acquired in a Bluetooth enabled data capture device,
7.2.1	wherein the new-data is data acquired by the Bluetooth enabled data capture device after establishing a paired Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth

	enabled cellular phone,
7.2.2	wherein establishing the Bluetooth paired connection comprises the Bluetooth enabled data capture device cryptographically authenticating an identity of the Bluetooth enabled cellular phone,
7.3.1	wherein detecting and receiving new-data acquired in the Bluetooth enabled data capture device comprises: said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection,
7.3.2	wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone; and
7.3.3	said mobile software application for the Bluetooth enabled cellular phone configured to receive, from the Bluetooth enabled data capture device, the event notification and the acquired new-data over the established paired Bluetooth connection;
7.4	store the received new-data in a memory of the Bluetooth enabled cellular phone;
7.5.1	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,
7.5.2	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
7.6	display a mobile advertisement inside the mobile software application.
8.	The mobile software application of claim 7, wherein the user authentication credential is stored in the memory of the Bluetooth enabled cellular phone, and wherein the user authentication credential is used by the remote server to authenticate a user.
9.	The mobile software application of claim 7, wherein the remote server is configured to store the new-data.
10.	The mobile software application of claim 7, wherein the mobile software application provides a touch based GUI for the received new-data.
11.	The mobile software application of claim 7, wherein the mobile software application provides a touch based advertisement targeted to a user.

12.P	A mobile software application for a Bluetooth enabled cellular phone comprising executable program instructions that, when executed by the processor controls the processor to:
12.1	detect and receive new-data acquired in a Bluetooth enabled data capture device,
12.2.1	wherein the new-data is data acquired by the Bluetooth enabled data capture device after establishing a paired Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone,
12.2.2	wherein establishing the Bluetooth paired connection comprises the Bluetooth enabled data capture device cryptographically authenticating an identity of the Bluetooth enabled cellular phone,
12.3.1	wherein detecting and receiving new-data acquired in the Bluetooth enabled data capture device comprises: said mobile software application for the Bluetooth enabled cellular phone configured to poll the Bluetooth enabled data capture device for new-data, over the established paired Bluetooth connection,
12.3.2	wherein polling comprises sending a request to the Bluetooth enabled data capture device to check if the acquired new-data is available for transfer; and

12.3.3	said mobile software application for the Bluetooth enabled cellular phone configured to receive, from the Bluetooth enabled data capture device, the acquired new-data over the established paired Bluetooth connection;
12.4	store the received new-data in a memory of the Bluetooth enabled cellular phone;
12.5.1	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,
12.5.2	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
12.6	display a mobile advertisement inside the mobile software application.
13.	The mobile software application of claim 12, wherein the user authentication credential is stored in the memory of the Bluetooth enabled cellular phone, and wherein the user authentication credential is used by the remote server to authenticate a user.
14.	The mobile software application of claim 12, wherein the remote

	server is configured to store the new-data.
15.	The mobile software application of claim 12, wherein the mobile software application provides a touch based GUI for the received new-data.
16.	The mobile software application of claim 12, wherein the mobile software application provides a touch based advertisement targeted to a user.

APPENDIX A

David B. Lett mobile (770) 335-8119 lettinnovations@gmail.com www.linkedin.com/in/David-Lett

Expert Witness, CTO

Technology industry veteran with electronics/software/hardware/video/audio/data expertise.
IoT | Consumer Electronics | Telecommunications | Cable | Satellite | Broadband |Wireless

- Expert witness testimony, technical consulting, and expert reports for renowned patent law firms such as Fish & Richardson and Banner Witcoff.
- 86 Patents and Patent publications. Served on corporate patent boards and as 30(b)(6) witness.
- Uniquely broad hardware/software/systems technical understanding.
- Award winning design and development including Best of Show, Technology Emmy, and Best of Innovations of over 100 million shipped products, responsible for $1.3B annual revenue.
- Industries: Consumer Electronics, Cable, Satellite, Internet of Things (IoT), Telematics, Smart Truck Logistics, Transportation, Alarm Systems, Smart Tank monitoring & fulfillment, Television, Telecommunications, Video, Audio, Wireless, Broadband, OTT Video, IPTV, Payments
- Technical: hardware design, software design, systems design, mechanical design, embedded systems, cloud computing, AWS, Azure, OCS, SaaS, fog computing, edge computing, high speed digital, C, Java, Linux, mobile applications (IOS and Android), web applications (Java, JavaScript, HTML), firmware, RTOS, user interfaces, UI/UX, video, audio, data, RF, DSP, communications, cybersecurity, encryption, error correction coding, real-time systems, cable, CATV, DOCSIS, broadband, satellite, satcom, IPTV, OTT video, video streaming, wireless, cellular, 3G, 4G, LTE, LTE-M, 5G, NB-IoT, Cat-M1, WiFi, ZigBee, Z-Wave, Bluetooth, LoRa, Internet of Things (IoT), IIoT, Machine-to-Machine (M2M), Telematics, AI, ML, networks, payments, consumer electronics, and telecommunications.

EXPERIENCE

Nov. 2016-present**, Expert Witness/CTO**, Independent Consultant
Technology, product development, organizational, & intellectual property consulting

- Expert Witness Reports - Declarations, Opinions, Inter Partes Review (IPR) Petitions and Defense
- Expert Witness Testimony - Depositions, Arbitrations, Trials
- Intellectual Property/Patent assistance, prosecution/defense strategy, search
- Technical Consulting

Jul. 2019 – June 2022, **Chief Technology Officer (CTO), Telular**, an Ametek Company**,** Greater Atlanta Area

- Responsible for global engineering, corporate technical strategy, and technical representation.
- Developed SaaS, mobile, and hardware products for Industrial IoT (IIoT) businesses including transportation, tank monitoring, petroleum logistics, and facility alarm monitoring with 1.4M+ subscribers, sold under the SkyBitz and Telguard brands.
- Led the development of an IoT Toolkit (scalable platform and APIs) to extend the Telular IoT platform for all 60+ (and growing) AMETEK companies, enabling development of high- value IIoT recurring revenue web and mobile applications.
- SaaS, Cellular, 3G, 4G, LTE, LTE-M, 5G, NB-IoT, Cat-M1, BLE, Satellite, cloud, distributed systems, Azure, Oracle Cloud, IoT, AI, ML, M2M, hardware, GPS, solar, low-power design, broadband, firmware, software, systems, architecture, video, mobile apps, web apps.

Aug. 2011 – Oct. 2016, **Vice President of Engineering, Head of the Atlanta R & D Center, EchoStar Technologies**, Greater Atlanta Area ($3B revenue, Engineering for Dish Network with a common controlling stockholder)

- Developed products for Dish Network and international customers including highest volume set-top boxes, H.265, HEVC, 3D, Satellite, MoCA, transcoding, Embedded C Linux applications, mobile applications (IOS and Android), SaaS, and web applications (Javascript, HTML). Provided product lifecycle support of contract manufacturers, test methodologies, customer service, QA, marketing, and sales.

- Led the architecture and global development of a huge end-to-end secure IoT cloud/fog/edge Platform for the consumer security & smart home market and other adjacent markets. Established the unique TV and mobile UI and MyLocal911 patented self-monitored security paradigm. System architecture consisted of 32 cloud systems and 24 CPE products. Systems included BSS/OSS, AWS cloud storage, 2-way video/audio streaming, authentication, provisioning, software download, command and control, customer service, online storefront, 911 emergency VoIP, logistics, CPE, and mobile applications. Represented the platform at trade shows.
- Functioned as a general manager in roles and responsibilities including vision, operations, business results, product management, program management, complex projects and services, hardware/software/systems product development of video, Internet of Things (IoT), and mobile application products.
- **Winner of the prestigious Best of Show award at the 2013 CES for the Hopper** because of the Hopper Transfers functionality and mobile applications.
- **Won 2015 CSI award "Best smart home product, technology or service".**

Aug. 1990 – July 2011, **Vice President of Engineering, Cisco / Scientific Atlanta**, Greater Atlanta Area
($35B / $1.9B revenue companies respectively. Cisco acquired Scientific Atlanta Feb. 2006)

- Intellectual property – served on the corporate patent board, provided patent assistance, and testified in patent litigation cases including as a 30(b)(6) witness representing the corporation.
- Responsible for the hardware/firmware/software/mechanical/systems/architecture/ASIC requirements design and development of several generations of high volume set top boxes and other products with extensive data communications and multimedia capabilities and advanced features including DOCSIS 1/2/3 and hybrid gateways, 802.11, IPTV, DVR, cable modems, ADSL, VDSL, DVB-T/C/S, bootloaders, factory diagnostics, application frameworks, Nagra, DRMs, conditional access, secure microprocessors, device management, Android, Adobe Flash, Linux, DVD play/record, MPEG-4, MPEG-2, H.264, NTSC, PAL, DAVIC, MoCA, high-performance CPUs, cablecards, network processors, HDMI, multiple video/audio display interfaces, 2D/3D graphics, multiple RF tuners, and full spectrum tuners.
- Products developed supported worldwide video, audio, power supply, and regulatory standards.
- Developed products manufactured in company factories, contract manufacturers (CMs), Original Design Manufacturers (ODMs), and Joint Design Manufacturers (JDMs).
- Developed processes and practices to ensure success in high quality, high volume, low cost, and fast time-to-market product development.
- Architected Video-On-Demand (VOD) systems.
- Architected robust software download system to ensure network disaster recovery to avoid truck rolls. Received some of the **industries' first downloadable software patents and an electronic program guide patent**. Developed the downloadable software system, enabling the applications software development business which evolved into a major corporate strategic business objective.
- Responsible for the total value proposition strategy internally in the organization through process design and externally facing customers to propose innovative solutions that add value and differentiate our offering.
- Established and managed department capex and opex budgets and manpower planning.
- Achieved unprecedented 3%/qtr product cost reductions for all products during the product lifecycle.
- Highly reliable products never had a field recall, which would have been disastrous to the business due to truck roll costs.
- Established software development department and software development practices including software processes, code reviews, networked version control and defect tracking, unit test teams, coding standards, and release processes.
- Reduced product development time to market for set top boxes from 14 months to 6 months through continuous process improvement
- Scaled organization from supporting $10M to $1.3B in sales
- Accounted for more than **70% of the revenues for Cisco's Service Provider Video Technology Group and for Scientific Atlanta Corporation**.
- Award winning design and development of over 100 million shipped products
- **Winner of Technology Emmy in 2012 for Pioneering Development of Multi-Room DVR.**

- **Winner of 2006 CES "Best of Innovations" award for DVR/DVD Recorder/Player.**
- **Winner of Motorola/EE Times Excellence in Innovation Award** in 1994.

Nov. 1985 - July 1990, **Hardware Engineering Manager / Senior Engineer, Wegener Communications, Inc.,** Greater Atlanta Area

- Managed product development of video, audio, and data satellite receivers, modulators, graphics display systems, DSP-based compandors, FSK and PSK satellite modems, multiplexers, forward error correction (FEC) codecs, RF upconverters and downconverters, and baseband analog and digital processing components. Disciplines managed included hardware, ASICs, FPGAs, RF, digital, microprocessors, analog, mechanical, and embedded software.
- Architected and designed forward error correction (FEC) coding systems, PSK modems, and analog control systems for RF modulators and PSK demodulators.

Mar. 1983 - June 1985 (while working at Scientific Atlanta), Assistant Professor, **DeVry Institute of Technology**, Greater Atlanta Area

- Taught evening school courses in microprocessor hardware/software and Electronics

June 1982 – Oct. 1985, **Scientific-Atlanta, Engineer II/Engineer I,** Greater Atlanta Area

- Designed software and hardware including addressable data transmitters, video sync suppression scramblers, transaction format converters, and data channel monitors for addressable Cable Television systems and Set Top Boxes.

EDUCATION

- MSEE course work in Electrical Engineering, Georgia Institute of Technology, Atlanta, Georgia
- BSEE, University of Tennessee, Knoxville, Tennessee, with High Honors. Specialization in Computer Engineering. GPA: 3.53/4.00.
- Georgia Institute of Technology Scrum Leadership Certificate, Certified Scrum Master (CSM), Certified Scrum Product Owner (CSPO), Certified Large Scale Scrum (LeSS) Practitioner
- Many short courses in business and engineering.