UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

64188 7590 09/14/2021

ASHOK TANKHA
36 GREENLEIGH DRIVE
SEWELL, NJ 08080

EXAMINER
NOORISTANY, SULAIMAN

ART UNIT	PAPER NUMBER
2415	

DATE MAILED: 09/14/2021

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/532,507	08/06/2019	Gurvinder Singh	CellSpin_04Con17_US	6207

TITLE OF INVENTION: Automatic Multimedia Upload For Publishing Data And Multimedia Content

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	12/14/2021

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

64188 7590 09/14/2021
ASHOK TANKHA
36 GREENLEIGH DRIVE
SEWELL, NJ 08080

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/532,507	08/06/2019	Gurvinder Singh	CellSpin_04Con17_US	6207

TITLE OF INVENTION: Automatic Multimedia Upload For Publishing Data And Multimedia Content

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	12/14/2021

EXAMINER	ART UNIT	CLASS-SUBCLASS
NOORISTANY, SULAIMAN	2415	370-313000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/532,507	08/06/2019	Gurvinder Singh	CellSpin_04Con17_US	6207

64188 7590 09/14/2021

ASHOK TANKHA
36 GREENLEIGH DRIVE
SEWELL, NJ 08080

EXAMINER	
NOORISTANY, SULAIMAN	
ART UNIT	PAPER NUMBER
2415	

DATE MAILED: 09/14/2021

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

LifeScan, Inc. Ex. 1006
Page 3 of 353
IPR2025-00102

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

LifeScan, Inc. Ex. 1006
Page 4 of 353
IPR2025-00102

Notice of Allowability	Application No. 16/532,507	Applicant(s) Singh et al.	
	Examiner SULAIMAN NOORISTANY	Art Unit 2415	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 9/6/21.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are 1-6,8-9 and 12-13 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information , please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☑ Interview Summary (PTO-413), Paper No./Mail Date. 9/3/21.
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/SULAIMAN NOORISTANY/
Primary Examiner, Art Unit 2415

Amendments to the claims

Claim 1 (currently amended): A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device;

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, 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, wherein the

LifeScan, Inc. Ex. 1006
Page 6 of 353
IPR2025-00102

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

Claim 2 (previously presented): 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.

Claim 3 (previously presented): 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.

LifeScan, Inc. Ex. 1006
Page 7 of 353
IPR2025-00102

Claim 4 (currently amended): A system, comprising:

a short-range wireless enabled data capture device, comprising:

a first memory device;

a first processor coupled to the first memory device;

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;

a data capture circuitry;

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;

said first processor further configured to store the new-data in the first memory device; and

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

LifeScan, Inc. Ex. 1006
Page 8 of 353
IPR2025-00102

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;

said short-range wireless enabled cellular phone, comprising:

a second memory device;

a second processor coupled to the second memory device;

a cellular network communication device configured to connect to the internet via a cellular data network;

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;

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, wherein the single mobile client application for the short-range wireless enabled cellular phone is configured to process the event notification;

receive the new-data from the short-range wireless enabled data capture device;

store the received new-data in the second memory device;

5

LifeScan, Inc. Ex. 1006
Page 9 of 353
IPR2025-00102

store a user authentication credential in the second memory device;

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 ~~at least one of~~ no wait automatic[[,]] or wait X minutes automatic~~, and wait for user input~~;

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

provide a touch based graphical user interface for the received new-data.

Claim 5 (previously presented): 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.

Claim 6 (previously presented): The system of claim 4, wherein the user authentication credential is for a user of the user data publishing website.

Claim 7 (cancelled).

Claim 8 (currently amended): A short-range wireless enabled cellular phone, comprising:

a memory device;

LifeScan, Inc. Ex. 1006
Page 10 of 353
IPR2025-00102

a processor coupled to the memory device;

a cellular network communication device configured to connect to internet via a cellular data network;

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;

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:

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;

receive the event notification and the new-data from the short-range wireless enabled data capture device;

process the event notification and store the received new-data in the memory device;

store a user authentication credential in the memory device;

LifeScan, Inc. Ex. 1006
Page 11 of 353
IPR2025-00102

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;

further use the HTTP to upload the received new-data and the user authentication credential to [[a]] 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 ~~at least one of~~ no wait automatic[[,]] or wait X minutes automatic~~, and wait for user input~~; and

provide a touch based graphical user interface for the received new-data.

Claim 9 (previously presented): The short-range wireless enabled cellular phone of claim 8, 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.

Claims 10-11 (cancelled).

Claim 12 (currently amended): A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device of the short-range wireless enabled data capture device;

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, 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;

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,

LifeScan, Inc. Ex. 1006
Page 13 of 353
IPR2025-00102

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 [[a]] the user data publishing website over [[a]] 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 ~~at least one of~~ no wait automatic[[,]] or wait X minutes automatic~~, and wait for user input~~, 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.

Claim 13 (previously presented): The short-range wireless enabled data capture device of claim 12, 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.

Claim 14 (cancelled).

LifeScan, Inc. Ex. 1006
Page 14 of 353
IPR2025-00102

Remarks

The pending claims

Claims 1-6, 8-9 and 12-13 are currently pending. Reconsideration and allowance of the pending claims is respectfully requested.

Summary of telephone conversation on September 3, 2021

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

Follow up by the applicant

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

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case. In the interest of compact prosecution, if the prosecution of the application can be advanced, applicant requests Examiner Nooristany to call the undersigned with the proposed amendment.

Respectfully submitted,

Date: September 6, 2021

/Ash tankha/
Ashok Tankha
Attorney For Applicant
Reg. No. 33,802

Correspondence Address

LifeScan, Inc. Ex. 1006
Page 15 of 353
IPR2025-00102

Ashok Tankha
Lipton, Weinberger & Husick
36 Greenleigh Drive
Sewell, NJ 08080
Fax: 856-374-0246
Phone: 856-266-5145
Email: ash@ipprocurement.com

LifeScan, Inc. Ex. 1006
Page 16 of 353
IPR2025-00102

Doc code. RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	16/532,507	Filing Date	2019-08-06	Docket Number (if applicable)	CellSpin_04Con17_US	Art Unit	2415
First Named Inventor	Gurvinder Singh			Examiner Name	Nooristany, Sulaiman		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____ (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 600314

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

X Patent Practitioner Signature

Applicant Signature

EFS - Web 2.1.16

LifeScan, Inc. Ex. 1006
Page 17 of 353
IPR2025-00102

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/ash tankha/	Date (YYYY-MM-DD)	2021-09-01
Name	Ashok Tankha	Registration Number	33802

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Amendments to the claims

Note: This claim set replaces the claim set submitted with the response to final office action submitted on June 22, 2021.

Amendments to the claims

Claim 1 (currently amended): A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device;

LifeScan, Inc. Ex. 1006
Page 20 of 353
IPR2025-00102

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, 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, 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, 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, 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, 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, wherein the upload is based on a timer setting on the single mobile client application, wherein the timer setting is at least one of no wait automatic, wait X minutes automatic, and wait for user input, and wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data.

Claim 2 (previously presented): 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.

LifeScan, Inc. Ex. 1006
Page 21 of 353
IPR2025-00102

Claim 3 (currently amended): 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.

Claim 4 (currently amended): A system, comprising:

a short-range wireless enabled data capture device, comprising:

a first memory device;

a first processor coupled to the first memory device;

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;

a data capture circuitry;

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;

said first processor further configured to store the new-data in the first memory device; and

LifeScan, Inc. Ex. 1006
Page 22 of 353
IPR2025-00102

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;

said short-range wireless enabled cellular phone, comprising:

a second memory device;

a second processor coupled to the second memory device;

a cellular network communication device configured to connect to the internet via a cellular data network;

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;

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, wherein the single mobile client application for the short-range wireless enabled cellular phone is configured to process the event notification;

receive the new-data from the short-range wireless enabled data capture device;

store the received new-data in the second memory device;

store a user authentication credential in the second memory device;

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 at least one of no wait automatic, wait X minutes automatic, and wait for user input; and

provide a touch based graphical user interface for the received new-data.

Claim 5 (previously presented): 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.

Claim 6 (previously presented): The system of claim 4, wherein the user authentication credential is for a user of the user data publishing website.

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

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

Claim 8 (currently amended): A short-range wireless enabled cellular phone, comprising:

a memory device;

a processor coupled to the memory device;

a cellular network communication device configured to connect to internet via a cellular data network;

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;

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:

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;

LifeScan, Inc. Ex. 1006
Page 25 of 353
IPR2025-00102

receive the event notification and the new-data from the short-range wireless enabled data capture device;

process the event notification and store the received new-data in the memory device;

store a user authentication credential in the memory device;

use HTTP to upload the received new-data and the user authentication credential to a user data publishing web service 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 at least one of no wait automatic, wait X minutes automatic, and wait for user input; and

provide a touch based graphical user interface for the received new-data.

Claim 9 (previously presented): The short-range wireless enabled cellular phone of claim 8, 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.

Claims 10-11 (cancelled).

Claim 12 (currently amended): A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

LifeScan, Inc. Ex. 1006
Page 26 of 353
IPR2025-00102

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device of the short-range wireless enabled data capture device;

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, 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;

9

LifeScan, Inc. Ex. 1006
Page 27 of 353
IPR2025-00102

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 upload the received new-data and the user authentication credential to a user data publishing website over a cellular data network, wherein the upload is based on a timer setting on the single mobile client application, and wherein the timer setting is at least one of no wait automatic, wait X minutes automatic, and wait for user input, 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.

Claim 13 (previously presented): The short-range wireless enabled data capture device of claim 12, 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.

Claim 14 (previously presented): The short-range wireless enabled data capture device of claim 12, wherein the mobile client application for the short-range wireless enabled cellular phone uses HTTP to send user preferences to the user data publishing web service over the cellular data network, wherein the user preferences comprise global positioning system information.

LifeScan, Inc. Ex. 1006
Page 28 of 353
IPR2025-00102

Remarks

The pending claims

Claims 1-9 and 12-14 are currently pending. Reconsideration and allowance of the pending claims is respectfully requested.

Summary of the Office Action

Summary of examiner interview on 07 May 2021

Applicant thanks the examiner for providing a telephonic interview on 07 May 2021. During the interview, an overview of the invention was presented and claims were discussed, but no formal agreement was reached.

Summary of examiner interview on 05 August 2021

During the interview, an overview of the invention was presented and proposed claim amendments were discussed, which examiner indicated appear to overcome the outstanding grounds of rejection and put the application in forward status. However, no formal agreement was reached during the interview.

Claim Rejections - 35 USC § 112

Claims 7, 14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

Specification Objection

The disclosure is objected to because of the following informalities: Examiner has reviewed the specification of this application under examination and could not find

LifeScan, Inc. Ex. 1006
Page 29 of 353
IPR2025-00102

support for the additional limitations as claimed "use HTTP to send user preference to the user data publishing website over the cellular data network, wherein the user preference comprise global positioning system information". Appropriate correction is required.

Claim Rejections - 35 USC § 112

Claims 7, 14 are rejected under 112, second paragraphs being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention.

Claim Rejections 35 U.S.C. 103

Claim 1-6, 8-9, 12-13 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778.

Claim 7 & 14 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778 further in view of Risbood US20070111748.

Amendments to the claims

Claims 1, 3-4, 8 and 12 are currently amended; claims 2, 5-7, 9 and 13-14 remain as previously presented; claims 10-11 were previously cancelled. Applicant respectfully submits that the amendments to the claims do not add any new subject matter.

Support for claim amendments

Support for the amendments: "*wherein the upload is based on a timer setting on the single mobile client application, and wherein the timer setting is at least one of no wait automatic, wait X minutes automatic, and wait for user input*" in claim 1 is found in

LifeScan, Inc. Ex. 1006
Page 30 of 353
IPR2025-00102

FIGS. 2, 4, page 11 line 12 to page 12, line 31, page 13, lines 9-12, page 14, lines 14-23, and page 16, lines 24-26 of applicant's originally filed application.

Support for the limitation: "*use HTTP to send user preferences to the user data publishing website over the cellular data network, wherein the user preferences comprise global positioning system information*" in claim 7 is found in:

(a) Point No. 2 of "CROSS REFERENCE TO RELATED APPLICATIONS" in the originally filed application, which states as follows: "*The following patent application is* ***incorporated herein in its entirety****: US Non-provisional patent application serial number 11/901,802, titled "Online Publishing of Multimedia Content", filed on September 19, 2007 in the United States Patent and Trademark Office." USPTO Publication No. 2008/0103906 A1 is the published application of US Non-provisional patent application serial number 11/901,802. US Non-provisional patent application serial number 11/901,802 is attached to the response to previously submitted response to non-final office action as Exhibit A and USPTO Publication No. 2008/0103906 A1 is attached to the previously submitted response to non-final office action as Exhibit B; see also link: https://patentimages.storage.googleapis.com/1f/06/a0/32f9a69fbef2a6/US20080103906A.pdf.*"

(b) Paragraph [0023] of Exhibit B, which states: "*The multimedia object is published 108 by the front end service 204b according to the user preferences on one or more publication virtual spaces 205 via the network 203.* ***The user preferences*** *may comprise* ***authentication credentials****, transaction identification,* ***a list of publication virtual spaces 205****,* ***global positioning system geographical codes****.*"

(c) Paragraph [0024] of Exhibit B, which states: "*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****.*"

LifeScan, Inc. Ex. 1006
Page 31 of 353
IPR2025-00102

(d) Paragraph [0028] of Exhibit B, which states: "*The preferences set by the user 201 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.* ***These user preferences are transferred to the publishing service 204."***

(e) Paragraph [0047] of Exhibit B, which states: "***The user 201 transfers*** *the* ***multimedia*** *object for publishing to a publication space selected by the user 201.* ***Additional information such as*** *the list of* ***the user preferences of the publication virtual spaces 205****,* ***authentication identification****, user preferences, default settings, manually entered* ***geographical codes****, and auction identifiers for eBay® and other shopping websites are selected 407 and* ***transferred along with the user created multimedia content to the publishing service 204***."

(f) Paragraph [0018] of Exhibit B, which states: "*The client application 202 communicates the user publishing information including the* ***user preferences of the publication virtual spaces 205*** *to the front end service 204b*", Paragraph [0023] of Exhibit B, which states: "*The* ***user preferences*** ***may comprise authentication credentials****, transaction identification,* ***a list of publication virtual spaces 205****,* ***global positioning system geographical codes***", Paragraph [0025] of Exhibit B, which states: "*The client application 202 enables the user 201 of the mobile device to record and transfer the user created multimedia content to the publishing service 204*", ***Paragraph [0061] of*** *Exhibit B, which states: "****The transport protocol that is used*** *between the client application 202 and the publishing service 204 may be* ***hypertext transfer protocol (HTTP)***".

The office action states: "**Claims 7, 14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The applicant fails to sufficiently point out or describe use of HTTP to send user**

LifeScan, Inc. Ex. 1006
Page 32 of 353
IPR2025-00102

preference to the user data publishing website over the cellular data network, wherein the user preference comprise global positioning system information."

In response to the above rejection, applicant submits that the recitation: "*use HTTP to send user preferences to the user data publishing website over the cellular data network, wherein the user preferences comprise global positioning system information*" in amended claim 7 is supported in the following paragraphs of Exhibit B:

(a) Paragraph [0018] of Exhibit B, which states: "The client application 202 communicates the user publishing information including the **user preferences of the publication virtual spaces 205** to the front end service 204b".

(b) **Paragraph [0023] of Exhibit B**, which states: "The **user preferences may comprise authentication credentials**, transaction identification, **a list of publication virtual spaces 205**, **global positioning system geographical codes**".

(c) Paragraph [0025] of Exhibit B, which states: "The client application 202 enables the user 201 of the mobile device to record and transfer the user created multimedia content to the publishing service 204".

(d) Paragraph [0061] of Exhibit B, which states: "The **transport protocol that is used** between the client application 202 and the publishing service 204 may be **hypertext transfer protocol (HTTP)".**

Applicant therefore respectfully submits that the following recitation in amended claim 7 is fully supported in Exhibit B:

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

LifeScan, Inc. Ex. 1006
Page 33 of 353
IPR2025-00102

Applicant therefore respectfully requests that the rejection of claim 7 under 35 U.S.C. 112, first paragraph be reconsidered and withdrawn.

Amended claim 14 is analogous to amended claim 7 and recites the same limitation as in amended claim 7. Applicant therefore respectfully requests that the rejection of claim 14 under 35 U.S.C. 112, first paragraph be reconsidered and withdrawn.

The office action further states: "**The disclosure is objected to because of the following informalities: Examiner has reviewed the specification of this application under examination and could not find support for the additional limitations as claimed "use HTTP to send user preference to the user data publishing website over the cellular data network, wherein the user preference comprise global positioning system information". Appropriate correction is required.**"

In response to the above objection, applicant submits that "*use HTTP to send user preference to the user data publishing website over the cellular data network, wherein the user preferences comprise global positioning system information*" is supported in the following paragraphs of Exhibit B:

(a) Paragraph [0018] of Exhibit B, which states: "The client application 202 communicates the user publishing information including the **user preferences of the publication virtual spaces 205** to the front end service 204b".

(b) Paragraph [0023] of Exhibit B, which states: "The **user preferences** may comprise **authentication credentials**, transaction identification, **a list of publication virtual spaces 205**, **global positioning system geographical codes**".

LifeScan, Inc. Ex. 1006
Page 34 of 353
IPR2025-00102

(c) Paragraph [0025] of Exhibit B, which states: "The client application 202 enables the user 201 of the mobile device to record and transfer the user created multimedia content to the publishing service 204".

(d) Paragraph [0061] of Exhibit B, which states: "The **transport protocol that is used** between the client application 202 and the publishing service 204 may be **hypertext transfer protocol (HTTP)**".

Applicant therefore respectfully submits that the objection to the specification be reconsidered and withdrawn.

The office action further states: "**Claims 7, 14 are rejected under 112, second paragraphs being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention. In claim 7, the terms "use HTTP to send user preference to the user data publishing website over the cellular data network, wherein the user preference comprise global positioning system information" are not clear what these are in reference to.**"

In response to the above rejection, applicant submits that "*use HTTP to send user preferences to the user data publishing website over the cellular data network, wherein the user preferences comprise global positioning system information*" is fully supported in the following paragraphs of Exhibit B:

(a) Paragraph [0018] of Exhibit B, which states: "The client application 202 communicates the user publishing information including the **user preferences of the publication virtual spaces 205** to the front end service 204b".

(b) Paragraph [0023] of Exhibit B, which states: "The **user preferences may comprise authentication credentials**, transaction identification, **a list of publication virtual spaces 205**, **global positioning system geographical codes**".

LifeScan, Inc. Ex. 1006
Page 35 of 353
IPR2025-00102

(c) Paragraph [0025] of Exhibit B, which states: "The client application 202 enables the user 201 of the mobile device to record and transfer the user created multimedia content to the publishing service 204".

(d) Paragraph [0061] of Exhibit B, which states: "The **transport protocol that is used** between the client application 202 and the publishing service 204 may be **hypertext transfer protocol (HTTP)**".

Applicant therefore respectfully requests that the rejection of claim 7 under 35 U.S.C. 112, second paragraph be reconsidered and withdrawn.

Amended claim 14 is analogous to amended claim 7 and recites the same limitation as in amended claim 7. Applicant therefore respectfully requests that the rejection of claim 14 under 35 U.S.C. 112, first paragraph be reconsidered and withdrawn.

The office action further states: "**Claim 1-6, 8-9, 12-13 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778.**"

In response to the above rejection, applicant submits that Hunter, in view of Pietruszka does not teach or suggest all the limitations in claims 1 and 12.

Arguments:

Argument#1:

Use HTTP to upload the received new-data and the user authentication credential to a user data publishing website over a cellular data network, where the upload is based on a timer setting on the single mobile client

application, and where the timer setting is at least one of no wait automatic, wait X minutes automatic, and wait for user input

Claim 1 discloses using HTTP to upload the received new-data and the user authentication credential to a user data publishing website over a cellular data network. Furthermore, claim 1 discloses that the upload is based on a timer setting on the single mobile client application.

By way of explanation, the website selection module **203g** of the media publishing module **203f** of a client application **203** shown in FIGS. **2**, **4** selects the websites for publishing the data and the multimedia content based on settings and user preferences configured by the user on the mobile device **202**. The timer module **203h** sets the time for publishing the transferred data and the multimedia content automatically or with minimal user intervention. The timer setting may be set for automatic publishing of the multimedia content or a time based wait mode where user interaction is required. The timer module **203h** sets the timer based on a timer setting, for example, a "no-wait-automatic" setting, a "wait-X-minutes-automatic" setting, and a "wait-X-minutes-user-input-cancel" setting configured by the user. The timer module **203h** ensures that if the user does not wish to publish the transferred data and multimedia content, the user has time to decide whether to publish or not. The user may also configure the client application **203** to automatically delete the data, the multimedia content, and the associated files after the data and the multimedia content have been posted and published on one or more websites based on user preferences.

The data transfer module **203j** transfers the data and the multimedia content from the client application **203** to the publishing service **401** via a network **402** for publishing on the websites automatically.

FIG. **4** exemplarily illustrates a system for publishing data and the multimedia content using a client application **203** on a mobile device **202** on one or more websites simultaneously. The client application **203** and a publishing service **401** are connected via

LifeScan, Inc. Ex. 1006
Page 37 of 353
IPR2025-00102

a network **402**. The client application **203** comprises a media publishing module **203f** as explained in the detailed description of FIG. **2**. The media publishing module **203f** comprises the website selection module **203g**, the timer module **203h**, the segmentation module **203i**, and the data transfer module **203j**. The website selection module **203g** selects the websites based on user preferences configured by the user on the mobile device **202**. The timer module **203h** sets the time for publishing the transferred data and the multimedia content automatically or with minimal user intervention. The timer module **203h** ensures that the publishing service **401** obtains the data, the multimedia content, and the associated files to publish on the selected websites based on the time set by the user.

The data transfer module **203j** transfers the data and the multimedia content from the client application **203** to the publishing service **401** via the network **402**.

The publishing service **401** comprises a front end service **401a**, a back end service **401b**, and a database **401d**. The transferred data and multimedia content is stored in the database **401d** of the publishing service **401**. A protocol is provided for synchronizing user publishing information between the client application **203** and the publishing service **401**. The user publishing information may, for example, comprise user preferences of the websites and the timer setting.

The back end service **401b** then creates a multimedia object from the transferred data and multimedia content. The multimedia object is transferred from the back end service **401b** to the front end service **401a** and then published on the websites selected by the user.

The client application **203** automatically publishes the transferred image on one or more websites via the internet **501**. The user **502** may set preferences in the mobile device **202**. The user preferences, for example, comprise the websites selected for publishing the transferred image. The user **502** may select websites, for example, Flickr™, Picasa™, YouTube™, eBay®, etc. and store the preferences on the mobile

LifeScan, Inc. Ex. 1006
Page 38 of 353
IPR2025-00102

device **202**. The user **502** may also set the timer setting for publishing the transferred image on the selected websites. After the captured image is transferred to the mobile device **202**, the client application **203** publishes the capture image on the selected websites based on the default timer and website settings configured by the user **502** on the mobile device **202**.

The transport protocol that is used between the client application **203** and the publishing service **401** may be hypertext transfer protocol (HTTP).

There is no teaching or suggestion in Hunter or Pietruszka of using HTTP to upload the received new-data and the user authentication credential to a user data publishing website over a cellular data network, where the upload is based on a timer setting on the single mobile client application.

In view of the above argument, Hunter in view of Pietruszka does not teach or suggest the following limitation in amended claim 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, 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, 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, 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, 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, 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, wherein the upload is based on a timer setting on the single mobile client application, wherein the timer setting is at least one of no wait automatic, wait X minutes automatic, and wait for user input, and wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data."

Argument#2:

The office action states that paragraph [0013] of Hunter is teaching the following limitation in claim 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, 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".

Applicant respectfully *disagrees* and submits the following arguments:

Hunter [0013]

LifeScan, Inc. Ex. 1006
Page 40 of 353
IPR2025-00102

[0013] In accordance with a fourth aspect of the invention, there is provided method of capturing and communicating images, comprising the steps of: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognising occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween; transferring images between the camera and the communications device over the wireless link; and transferring said images from the communications device on to a data network through a data network interface.

Recognizing ≠ Sending

In fact, it is the opposite of *sending*.



(a) In **Hunter** paragraph [0013], the Camera is ***recognizing*** **a trigger event**. In applicant's claim 1, the Camera is **Sending** an event notification.

(b) Recognizing an event trigger (Hunter) is not same as Sending an event notification in applicant's claim 1.

(c) Recognize is not the same as Sending

LifeScan, Inc. Ex. 1006
Page 41 of 353
IPR2025-00102

(d) In Hunter paragraph [0013], the Camera is recognizing a trigger event sent by the phone and then the camera is acquiring the image.

(e) In applicant's claim 1, the Camera is Sending an event notification, for the image that has already been acquired.

(f) In Hunter paragraph [0013], the "event trigger" is to acquire an image.

(g) In applicant's claim 1, the "event notification" corresponds to the image that has already been acquired.

(h) Receiving an Event trigger to acquire an image is not same as sending an event notification for the image already acquired.

Note: See extract of office action reproduced below and applicant's response:

said first processor further configured to send an event notification **(Hunter: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween [0013])** and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically **(Hunter: transferring images between the camera and the communications device over the wireless link [0013])**, 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 **(Hunter: [0013])**.

- In Hunter [0013] the Camera is **recognizing** a trigger event.
- In our claims the Camera is **Sending** an event notification.
- Recognize an event trigger ≠ Sending an event notification
- Recognize ≠ Sending

- In Hunter [0013] the Camera is **recognizing** a trigger event sent by the phone and then the camera is taking the image.
- In our claims the Camera is **Sending** an event notification, for the image that has *already been taken*.
- In Hunter [0013] the "event trigger" **is to take an image**
- In our case the "event notification" corresponds to the image that has *already been taken*
- Receiving an Event trigger to take an image ≠ sending an event notification for the image already taken.

Argument #3:

Furthermore, the office action states that paragraph [0025] of Hunter and paragraph [0099] of Pietruszka teach the following limitation in claim 1:

> "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."

Applicant respectfully *disagrees* and submits the following arguments:

(a) In Hunter paragraph [0025], the touch interface and operation is on the camera device and for the image acquired on/by the camera.

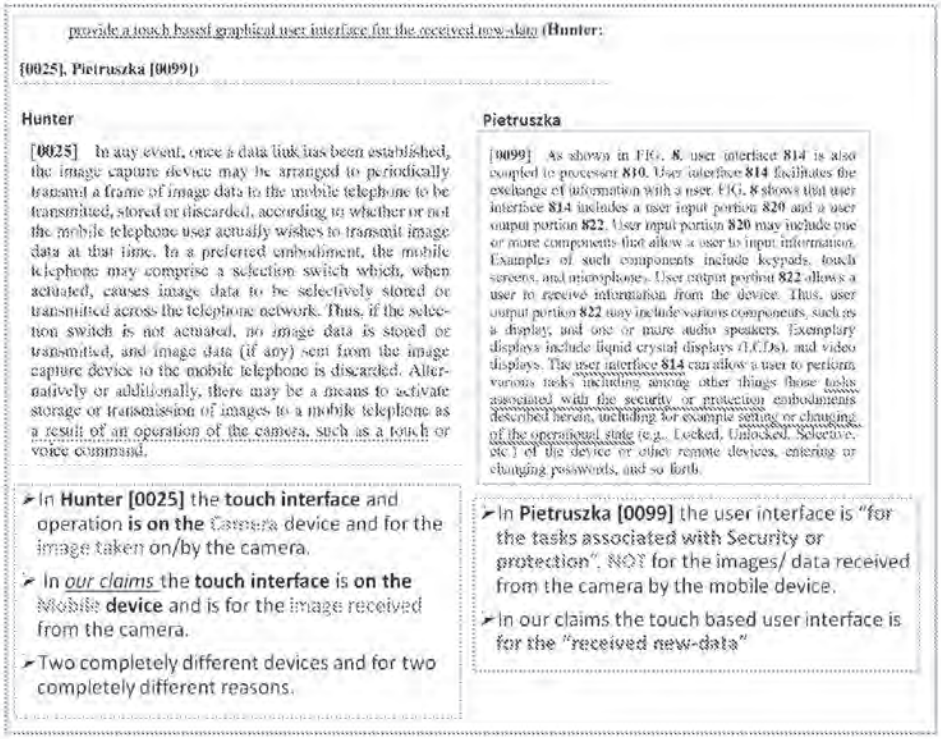
(b) In applicant's claim 1, the touch interface is on the mobile device and is for the image received from the camera.

(c) Two completely different devices and for two completely different reasons.

(d) In Pietruszka paragraph [0099], the user interface is "for the tasks associated with Security or protection"; NOT for the images/ data received from the camera by the mobile device'

(e) In applicant's claim 1, the touch based user interface is for the "received new-data".

Note: See extract of office action reproduced below and applicant's response:



Argument #4:

Furthermore, the office action states that paragraph [0037] and FIGS. **9A-9D** of Pietruszka teach the following limitation in claim 1:

> "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"

Applicant respectfully *disagrees* and submits the following arguments:

Paragraph [0037] of Pietruszka discloses cryptographically authenticating a short-range wireless device. In contrast, applicant's claim 1 recites storing of website "user"

authentication credentials on the mobile. Furthermore, FIGS. **9A-9D** disclose that the authentication is for the short-range wireless device and NOT for a website user.

Therefore, applicant submits that "*Cryptographic authentication of a wireless device*" in Pietruszka is not same as "*Website user authentication credentials*" as recited in applicant's claim 1.

To illustrate the point with an example, a *Facebook or YouTube website* ***"user authentication credential"*** is completely different from a cryptographic authentication being performed between & by *two devices* such as a camera and a mobile phone.

Note: See extract of office action reproduced below and applicant's response:

> **Pietruszka** further teaches cryptographically authenticating (**Pietruszka: [0037]**); store the user authentication credential in the second memory device (**Pietruszka fig. 9A-9D**) and

> **[0037]** A device that wishes to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt data exchanged over a wireless medium as an added security. The encryption can however be turned off and passkeys can be stored on the device's file system rather than the Bluetooth component or chip itself. Since the Bluetooth address can be permanent, a pairing can be preserved even if the Bluetooth name is changed. Either device in a pairing relationship may delete the pairing between the devices. Devices may require pairing or may prompt the user before it allows a remote device to utilize any or all or some of its services.

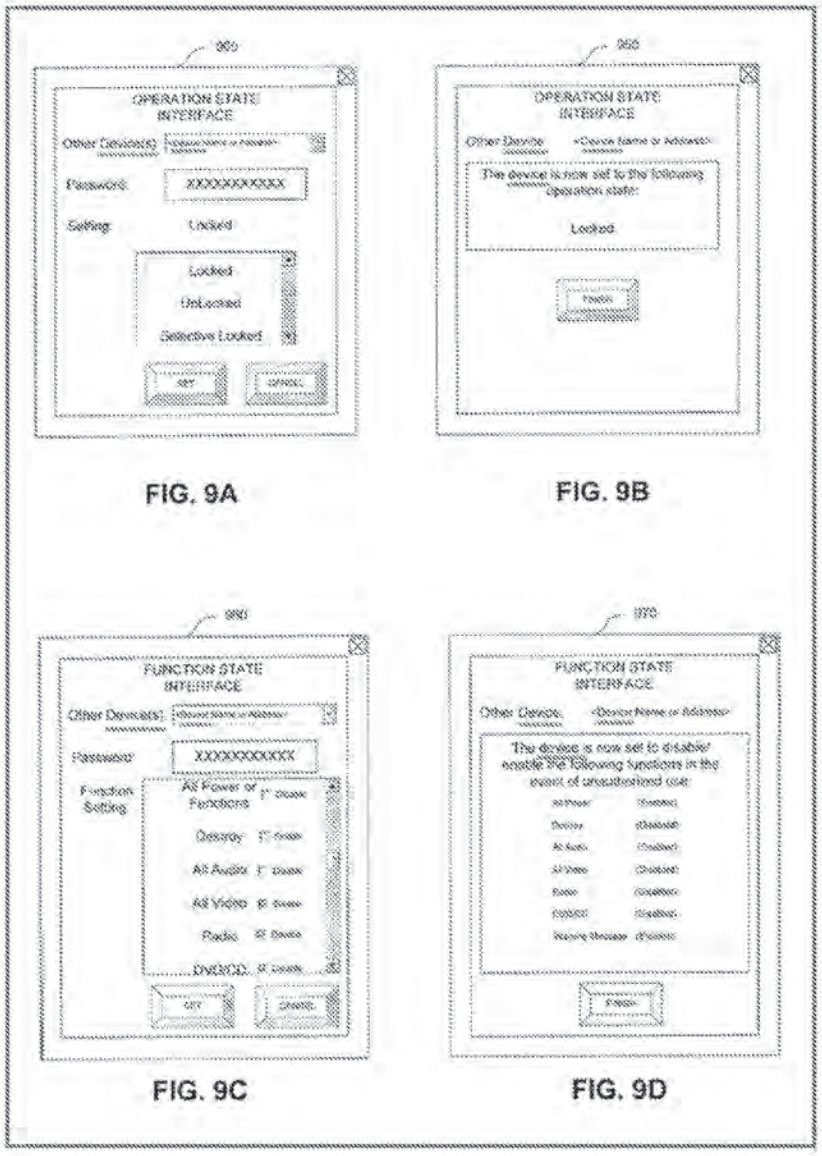


FIG. 9A

FIG. 9B

FIG. 9C

FIG. 9D

LifeScan, Inc. Ex. 1006
Page 47 of 353
IPR2025-00102

- In **Pietruszka [0037] is talking about cryptographically authenticating a short-range wireless device. Our Claim is about storing website "user" authentication credentials on the mobile!**
- In **Pietruszka [Fig 9A – 9D] make it clear that the authentication is for the Device and NOT a website user**

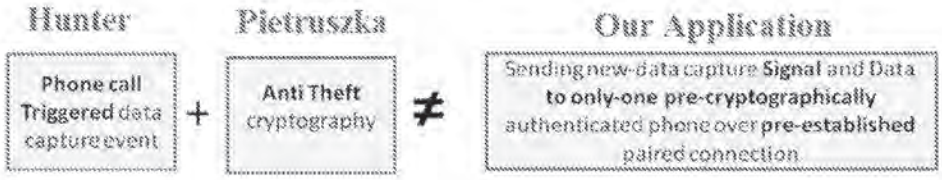
Cryptographic authentication of a wireless device

$\neq$

Website user authentication credentials

Argument #5:

Furthermore, there is no motivation to combine (i) Phone call triggered data capture event of Hunter with (ii) the Anti-Theft Pietruszka teaching.



Argument #6:

Establishment of non-paired connection (Hunter)

VS

Establishment of paired short-range Wireless (Applicant)

The office action on page 7 states that Hunter teaches the step of acquiring new-data 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. Applicant disagrees and presents the following arguments.

Hunter prior art does NOT teach pairing or paired connection. There is NO mention of word pair, pairing, paired in Hunter Specification. Short-range Pairing and Paired wireless connection are terms of short-range wireless technology and have been known and was used in the wireless industry for almost 10 years before the Cellspin patent's priority date of December 2007. Bluetooth wireless standard organization was the first to introduce the term "Bluetooth" at the Blackberry technology consortium in 1998; see Exhibit C, also available at the link: https://web.archive.org/web/20180525083558/https://www.bluetooth.com/about-us/our-history. Furthermore, in 1999, the detailed Bluetooth 1.0 specification with pairing was released; see Exhibit D attached to this response; also available at the link: http://grouper.ieee.org/groups/802/15/Bluetooth/profile_10_b.pdf.

The concept of a paired connection, as established by the Bluetooth Special Interest Group (Bluetooth SIG), became known and adopted by certain other industry organizations creating short-range wireless technology for device connections, such as WiFi Alliance and Zigbee Forum. In the context of short-range wireless connections, the term "pairing" was adopted by the wireless industry almost 10 years before the Cellspin patent's priority date of December 2007. Drawing from short-range wireless industry's understanding of the term "paired connection" / pairing, the broadest reasonable interpretation (BRI) of "paired connection" as understood by POSITA in Dec 2007, i.e., 10 years after the term was introduced in the wireless lexicon is:

> "bidirectional communications link between devices which provides for encrypted data exchange between the devices, and the communication link can be disconnected and reconnected without having to repeat pairing or authentication."

Because short-range "pairing" is a well-understood term in the art, the applicant followed Federal Court's direction that the "patent need not teach, and preferably omits,

what is well known in the art." See McRO, Inc. v. Bandai Namco Games Am. Inc., 959 F.3d 1091, 1102 (Fed. Cir. 2020). In conformance with this guidance, the applicant cited a version of "pairing" at least 50 times without explicitly defining it. Additionally, while not explicitly defining "pairing," the applicant provided guidance to a POSITA that short-range "pairing" should conform to Bluetooth's conception of the term, which was later adopted when ZigBee and WiFi adopted pairing, making it the only definition applicable to short-range paired wireless connections whether or not a Bluetooth Connection.

Argument #7:

Receiving or making Phone call trigger event (Hunter)

VS

NO such Phone call trigger event (Applicant)

The office action on page 6 states that Hunter teaches the step of acquiring new-data 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. Applicant disagrees and presents the following arguments.

The sequence of events in Hunter is as follows:

(i) Mobile device generates a trigger event or signal in response to a phone call received by the mobile device or a phone call made by the mobile device.

(ii) Send the trigger event or signal from the mobile device to the data capture device.

(iii) Only after receipt of the trigger event or signal from the mobile device, the data capture device acquires new-data and transmits the same to the mobile device for onward transfer to a website or web service.

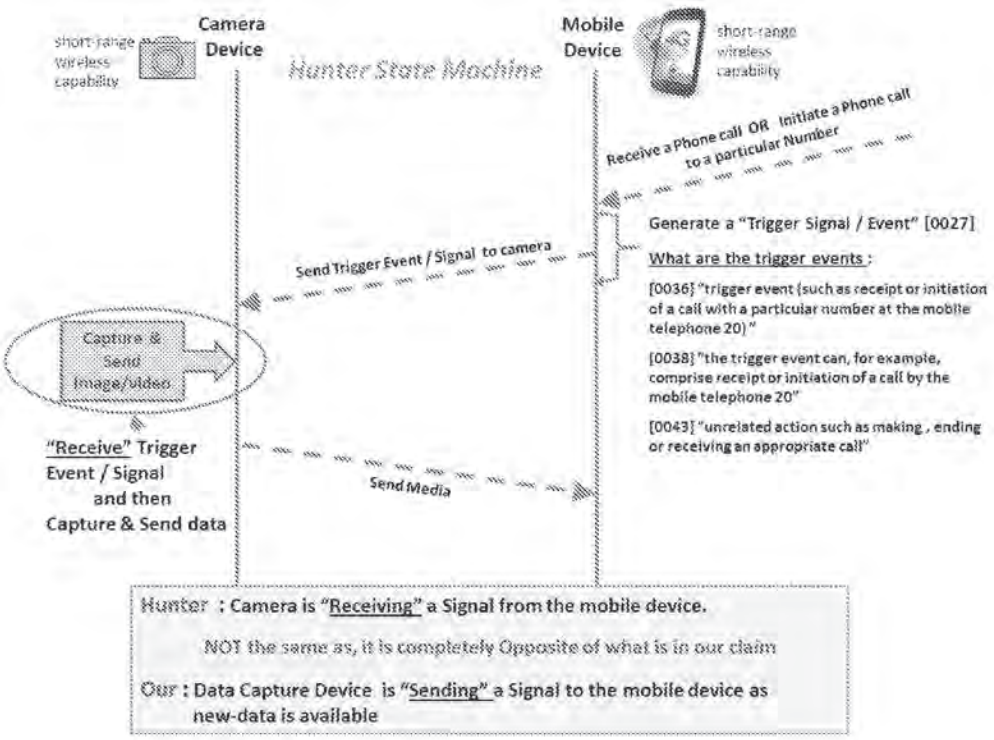
LifeScan, Inc. Ex. 1006
Page 50 of 353
IPR2025-00102

Firstly, in Hunter, there is NO pairing of the mobile device by the data capture device. Next, there is NO cryptographic authentication of the mobile device by the data capture device. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be sent to the data capture device.

Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where a data capture device acquires new-data after a short-range paired wireless connection is established with a cellular phone (without any phone call trigger event from the cellular phone to the data capture device).

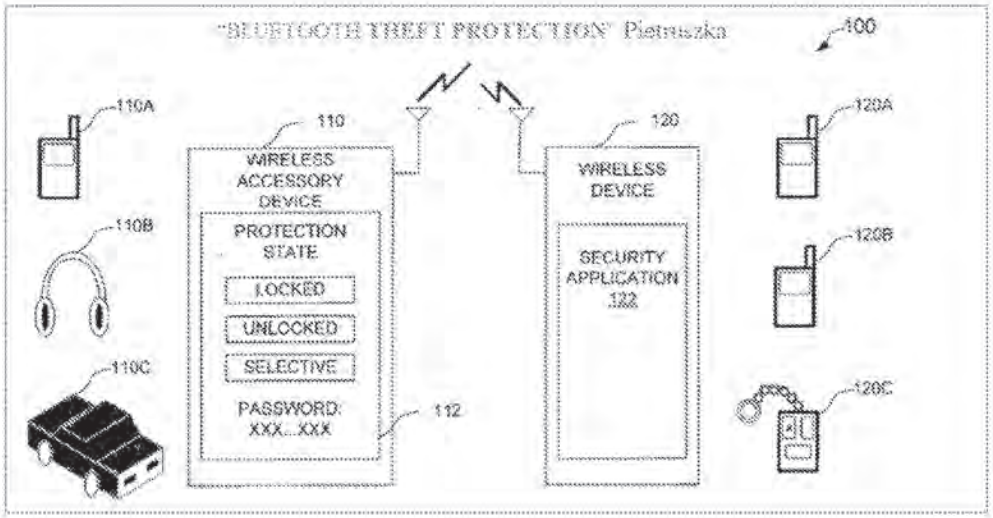
Next, in Hunter, the phone call trigger event is sent from the mobile device to the data capture device. This is in direct contrast to applicant's disclosure, where, after acquiring the new-data, the data capture device sends a notification signal to the mobile device informing the mobile device that it has acquired the new-data.

LifeScan, Inc. Ex. 1006
Page 51 of 353
IPR2025-00102



Argument #8:

Anti-Theft Pietruszka Setting based control of cryptographic pairing between devices is NOT relevant in applicant's scenario



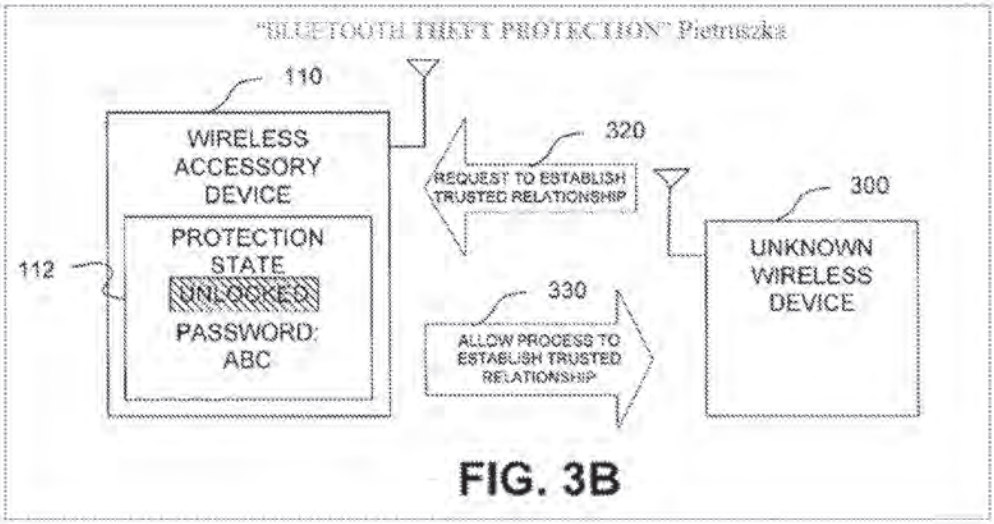


FIG. 3B

Pietruszka ("BLUETOOTH THEFT PROTECTION") discloses, inter alia, the following:

(a) User pre-selects whether or not a wireless communications device is allowed to establish a cryptographic pairing with a remote device.

(b) Control whether the wireless communications device is able to establish a cryptographic pairing with a remote device according to the pre-set operational state; see Pietruszka claim 1, and Paragraph [0005].

Pietruszka teaches mainly a setting-based control of cryptographic pairing between devices and it is not applicable in applicant's scenario. Applicant is NOT using a setting-based control for cryptographic pairing between devices.

Applicant is not implementing any Anti-theft technology. Applicant is not interested in a car or a key fob, or someone else hacking the car to steal it or the car accessories.

Pietruszka teaches mainly an Anti-theft technology and is not applicable in applicant's scenario. Applicant is NOT using pre-set operational state based cryptographic pairing for Anti-Theft purposes for car or car accessories.

Furthermore, in Pietruszka, car or a key fob is "NOT a data capture device" and does not send any data through the mobile phone to the internet.

In Pietruszka there is NO data capture device. Car or a key fob device described in Pietruszka is used as a theft control device. The Car or a key fob device is NOT capturing any data for transfer through the mobile device.

Furthermore, in Pietruszka, NO new-data is acquired for sending to the mobile phone after establishing the short-range paired wireless connection. Pietruszka's invention is all about the theft protection based on pre-set operational state of the device in its proximity.

Furthermore, there is NO Motivation to combine an anti-theft Pietruszka with Hunter to capture data and send data to a website using a cellphone.

LifeScan, Inc. Ex. 1006
Page 54 of 353
IPR2025-00102

In view of above arguments 2-8, applicant submits that Hunter, in view of Pietruszka does not teach or suggest the following limitations in claim 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, 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;"

> "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;"

Argument #9:

> **Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data.**

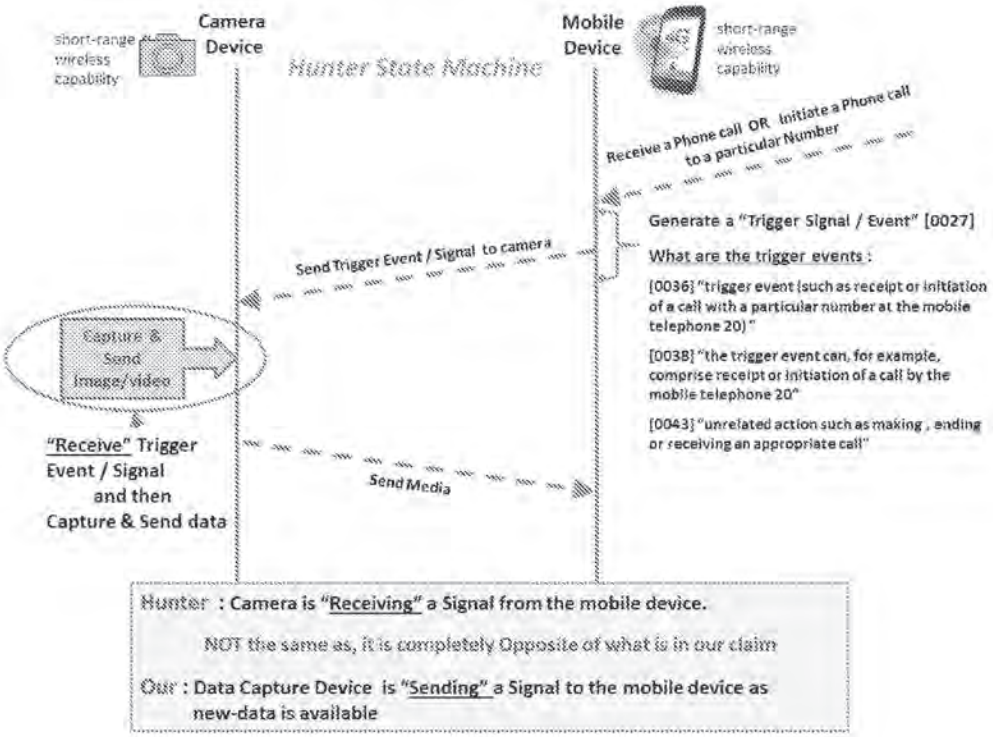
In claim 1, applicant discloses that after establishing the paired short-range wireless connection between the data capture device and the cryptographically authenticated short-range wireless enabled cellular phone, and after acquiring new-data, the short-range wireless enabled data capture device sends the event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone.

LifeScan, Inc. Ex. 1006
Page 55 of 353
IPR2025-00102

The office action on page 7 states that paragraph [0013] of Hunter teaches: "Sending an event notification to a cryptographically authenticated Bluetooth enabled cellular phone". Applicant disagrees and presents the following arguments.

Paragraph [0013] of Hunter states as follows: "programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween; transferring images between the camera and the communications device over the wireless link; and transferring said images from the communications device on to a data network through a data network interface."

Hunter state machine is again reproduced below to explain paragraph [0013]:



LifeScan, Inc. Ex. 1006
Page 56 of 353
IPR2025-00102

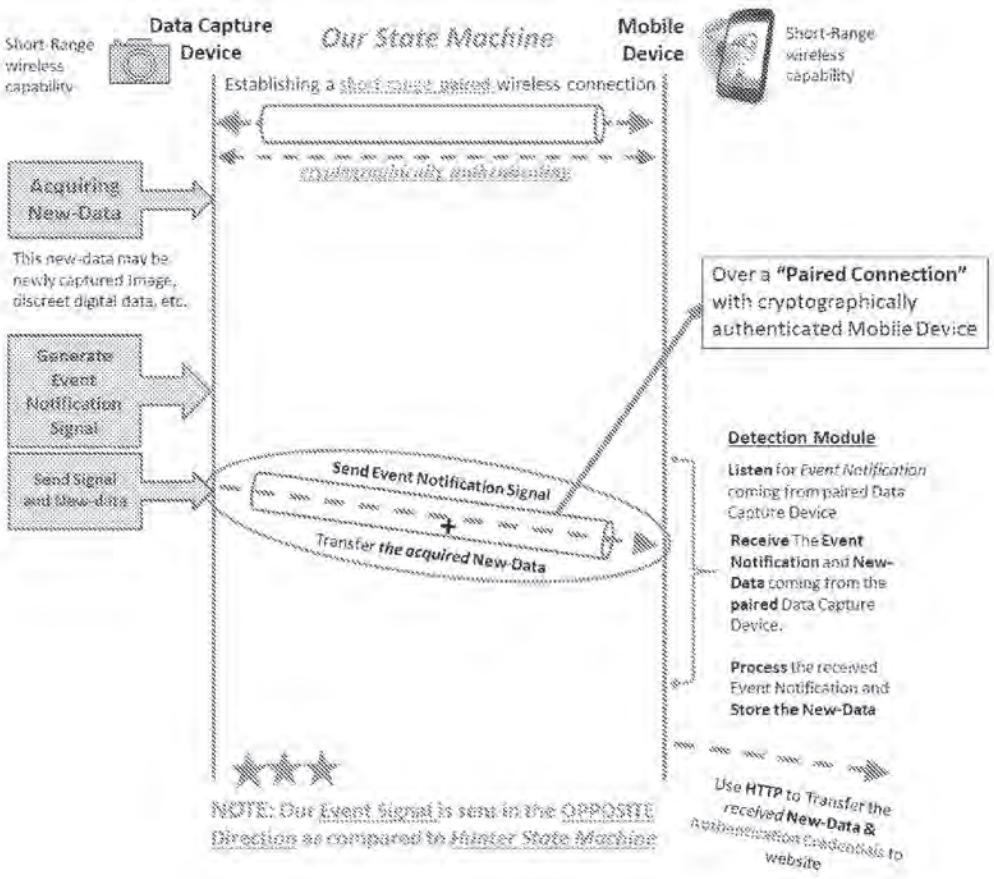
Firstly, in Hunter, there is NO cryptographic authentication of the mobile device by the data capture device before the signal is sent or the data is sent. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be sent to the data capture device.

Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where a data capture device acquires new-data after a short-range paired wireless connection is established with a cellular phone (without any phone call trigger event from the cellular phone to the data capture device).

Next, in Hunter, the phone call trigger event is sent from the mobile device to the data capture device. Event Signal is sent in the opposite direction when compared to the applicants claims. Direction of event signal is in direct contrast to applicant's disclosure, where, after acquiring the new-data, the data capture device sends a notification signal to the mobile device informing the mobile device that it has acquired the new-data.

In contrast, applicant's state machine is shown below.

LifeScan, Inc. Ex. 1006
Page 57 of 353
IPR2025-00102



Therefore, it is clear that the trigger notification in Hunter is not the same as the event notification in applicant's disclosure. Furthermore, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate the trigger event to be sent to the camera. Furthermore, in Hunter, the camera acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where the data capture device acquires new-data immediately after the paired short-range wireless connection is established (without any phone call trigger event from the mobile device). Furthermore, in Hunter, the trigger event or signal is sent from the mobile device to the camera, and image capture occurs after receiving the trigger event. This is in direct contrast to applicant's disclosure, where,

after acquiring the new-data, the data capture device sends the notification signal to the mobile device informing the mobile device that it has acquired the new-data.

Argument #10:

Phone call Trigger event in Hunter (see paragraphs [0036], [0038], [0043]) over NON paired connection

As illustrated before, in Hunter, there is no cryptographic authentication of the mobile device by the camera. Furthermore, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate the trigger event or signal to be sent to the camera. Furthermore, in Hunter, the camera acquires the new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where the data capture device acquires the new-data immediately after a paired short-range wireless connection is established (without any phone call trigger event from the mobile device). Furthermore, in Hunter, the phone call trigger event or signal is sent from the mobile device to the camera. This is in direct contrast to applicant's disclosure, where, after acquiring the new-data, the data capture device sends the notification signal and the acquired new-data to the mobile device.

In view of above arguments 9-10, and in view of argument 1, applicant submits that Hunter, in view of Pietruszka does not teach or suggest the following limitation in claim 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, 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, wherein the cryptographically authenticated short-range wireless enabled cellular phone is configured to listen to

41

LifeScan, Inc. Ex. 1006
Page 59 of 353
IPR2025-00102

the event notification and receive the new-data over the established short-range paired wireless connection, 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, 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, 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, wherein the upload is based on a timer setting on the single mobile client application, wherein the timer setting is at least one of no wait automatic, wait X minutes automatic, and wait for user input, and wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data."

Argument #11:

None of the cited prior art show the Claim 12 Polling limitation of:

Short-range wireless enabled cellular phone sends a polling request to a short-range wireless enabled data capture device, over an established paired short-range wireless connection, to detect new-data for transfer from the short-range wireless enabled data capture device to the paired and cryptographically authenticated short-range wireless enabled cellular phone

As illustrated before, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate the trigger event or signal to be sent to the

LifeScan, Inc. Ex. 1006
Page 60 of 353
IPR2025-00102

camera. Furthermore, in Hunter, the camera acquires the new-data only after it receives the trigger event or signal from the mobile device. In contrast, in applicant's disclosure, the polling request from the mobile phone to the camera is for detecting already acquired new data.

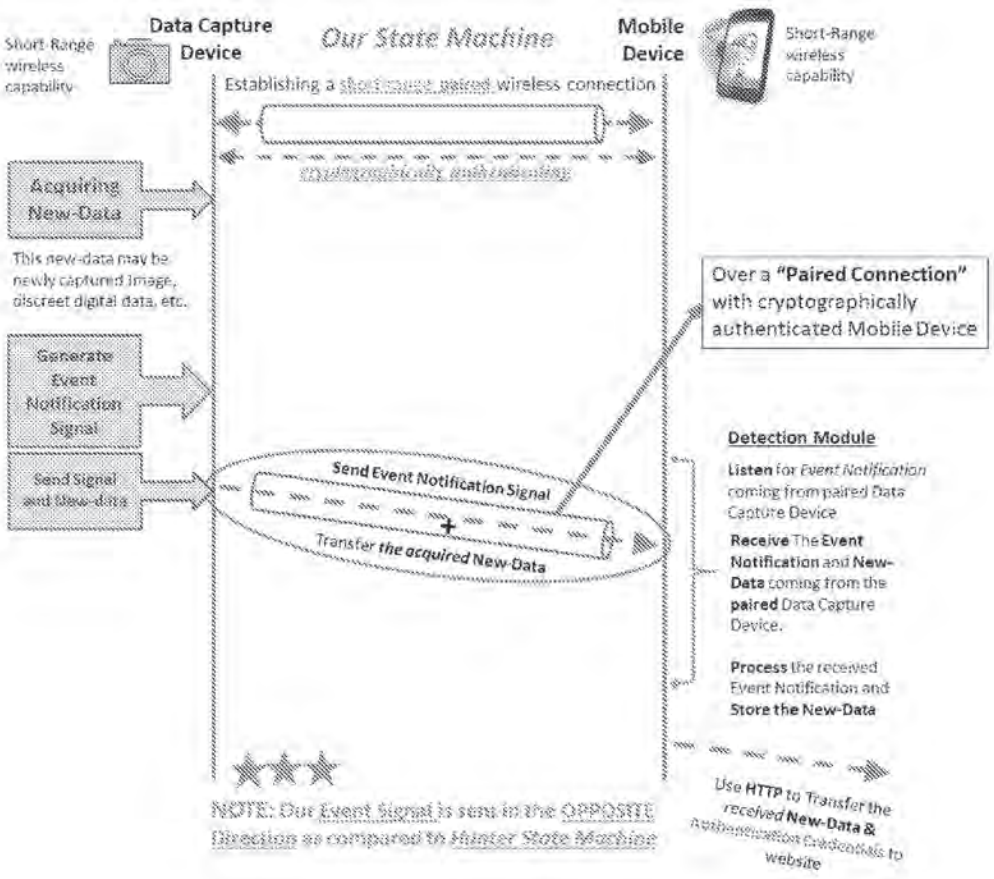
In view of above argument 11, applicant submits that Hunter, in view of Pietruszka does not teach or suggest the following limitation in claim 12:

> "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, 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;"

Summary

Applicant's state machine

LifeScan, Inc. Ex. 1006
Page 61 of 353
IPR2025-00102


Short-Range wireless capability
Data Capture Device
Our State Machine
Mobile Device
Short-Range wireless capability
Establishing a short-range paired wireless connection
cryptographically authenticated
Acquiring New-Data
This new-data may be newly captured image, discreet digital data, etc.
Generate Event Notification Signal
Send Signal and New-data
Over a "Paired Connection" with cryptographically authenticated Mobile Device
Send Event Notification Signal
+
Transfer the acquired New-Data
Detection Module
Listen for Event Notification coming from paired Data Capture Device
Receive The Event Notification and New-Data coming from the paired Data Capture Device.
Process the received Event Notification and Store the New-Data
Use HTTP to Transfer the received New-Data & Authentication Credentials to website
NOTE: Our Event Signal is sent in the OPPOSITE Direction as compared to Master State Machine

Comparison Table

	Claim Feature	Hunter	Pietruszka	Applicant Cellspin
1	Pairing for new-data transfer.	NO mention of pairing. Pairing is NOT established. Teaching away from establishing permanent connection.	NO Invention is about selecting or preventing, and controlling pairing between devices. NOT for new-data transfer	YES Pairing is established to transfer the acquired new-data.
2	Cryptographically authenticate the identity of Mobile Device	NO	YES Only if wireless communication device is unlocked for pairing.	YES The Mobile device is cryptographically authenticated by the data capture device NOT based on pre-selection of activation or deactivation of pairing.
3	Sending new data capture Event Notification Signal	NO Trigger Event Signal is sent from the mobile device to the camera device, which is opposite to applicant's invention.	NO There is NO data capture Event signal sent to the cellular phone. There is NO data capture device.	YES Event Notification signal is sent from data capture device to cellular phone after acquiring new-data.
4	Send data to the mobile device over a pre-established paired connection	NO	NO There is no data to transfer.	YES
4	HTTP based transfer	NO HTTP is NOT used	NO There is No data to transfer.	YES HTTP is used as a data transport protocol
5	Is Timing of Data Acquisition after Pairing devices	NO	NO	YES After pairing is established
6	Data transfer between two devices happens over what type of wireless link?	NON-Paired wireless connection	NO data There is no new- data to transfer	Data over Paired wireless connection

In view of the above arguments, Hunter, in view of Pietruszka does not teach or suggest all the limitations in claims 1 and 12. Furthermore, claims 1, 4, 8 and 12 are analogous to each other. Therefore, claims 1, 4, 8 and 12 are non-obvious over Hunter, in view of Pietruszka. Applicant therefore respectfully requests that the rejection of claims 1, 4, 8 and 12 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

Claims 2-3 are dependent on claim 1; claims 5-6 are dependent on claim 4; claim 9 is dependent on claim 8; claim 13 is dependent on claim 12. Applicant therefore respectfully submits that dependent claims 2-3, 5-6, 9 and 13 are also non-obvious over Hunter, in view of Pietruszka. Applicant therefore respectfully requests that the rejection

of claims 2-3, 5-6, 9 and 13 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

The office action further states: "**Claim 7 & 14 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778 further in view of Risbood US20070111748.**"

In an earlier part of this response, arguments were presented to show that the following limitations in amended claim 1 are not taught or suggested by Hunter, in view of Pietruszka:

> "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;"
>
> "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;"
>
> "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, 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, 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, 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, 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, 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, wherein the upload is based on a timer setting on the single mobile client application, wherein the timer setting is at least one of no wait automatic, wait X minutes automatic, and wait for user input, and wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data."

Risbood does not remedy the deficiencies in a combination of Hunter and Pietruszka. Therefore, the following limitations in amended claim 1 are not taught or suggested by Hunter, in view of Pietruszka and Risbood:

"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;"

"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;"

"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, 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, 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, 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, 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, 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, wherein the upload is based on a timer setting on the single mobile client application, wherein the timer setting is at least one of no wait automatic, wait X minutes automatic, and wait for user input, and wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data."

Claim 1 is therefore non-obvious over Hunter, in view of Pietruszka, further in view of Risbood. Claim 12 is analogous to claim 1. Therefore, claim 12 is therefore non-obvious over Hunter, in view of Pietruszka, further in view of Risbood. Claims 7 and 14 are dependent on claims 1 and 12 respectively. Since claims 1 and 12 are non-obvious over Hunter, in view of Pietruszka, further in view of Risbood, dependent claims 7 and 14 are also non-obvious over Hunter, in view of Pietruszka, further in view of Risbood. Applicant therefore respectfully requests that the rejection of claims 7 and 14 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

Furthermore, in view of "After Final Consideration Pilot 2.0 (AFCP 2.0) request" not being accepted, applicant submits, along with this response, a "Request for Continued Examination (RCE)" in compliance with 37 CFR 1.114, along with the RCE fee.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case. In the interest of compact prosecution, if the prosecution of the application can be advanced, applicant requests Examiner Nooristany to call the undersigned with the proposed amendment.

Respectfully submitted,

Date: September 01, 2021

/Ash tankha/
Ashok Tankha
Attorney For Applicant
Reg. No. 33,802

Correspondence Address
Ashok Tankha
Lipton, Weinberger & Husick
36 Greenleigh Drive
Sewell, NJ 08080
Fax: 856-374-0246
Phone: 856-266-5145
Email: ash@ipprocurement.com

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/532,507	08/06/2019	Gurvinder Singh	CellSpin_04Con17_US	6207

64188 7590 08/10/2021

ASHOK TANKHA
36 GREENLEIGH DRIVE
SEWELL, NJ 08080

EXAMINER	
NOORISTANY, SULAIMAN	

ART UNIT	PAPER NUMBER
2415	

NOTIFICATION DATE	DELIVERY MODE
08/10/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ASH@IPPROCUREMENT.COM
docketing1@ipprocurement.com
docketing@ipprocurement.com

PTOL-90A (Rev. 04/07)

LifeScan, Inc. Ex. 1006
Page 68 of 353
IPR2025-00102

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

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

Date of Interview: 05 August 2021

Issues Discussed:

Proposed Amendment(s)

During the interview, an overview of the invention was presented and proposed claim amendments were discussed, which Examiner indicated appear to overcome the outstanding grounds of rejection and put the application in forward status. However, no formal agreement was reached during the interview

/SULAIMAN NOORISTANY/ Primary Examiner, Art Unit 2415	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/532,507	08/06/2019	Gurvinder Singh	CellSpin_04Con17_US	6207

64188 7590 07/29/2021

ASHOK TANKHA
36 GREENLEIGH DRIVE
SEWELL, NJ 08080

EXAMINER
NOORISTANY, SULAIMAN

ART UNIT	PAPER NUMBER
2415	

NOTIFICATION DATE	DELIVERY MODE
07/29/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ASH@IPPROCUREMENT.COM
docketing1@ipprocurement.com
docketing@ipprocurement.com

PTOL-90A (Rev. 04/07)

LifeScan, Inc. Ex. 1006
Page 70 of 353
IPR2025-00102

Advisory Action Before the Filing of an Appeal Brief	Application No. 16/532,507	Applicant(s) Singh et al.	
	Examiner SULAIMAN NOORISTANY	Art Unit 2415	AIA (FITF) Status No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 22 July 2021 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☑ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires ____ months from the mailing date of the final rejection.
   b) ☑ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
   c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires ____ months from the mailing date of *the prior Advisory Action* or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.

   Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANTS FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   b) ☐ They raise the issue of new matter (see NOTE below);
   c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____ (See 37CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicants reply has overcome the following rejection(s): _____
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☑ For purposes of appeal, the proposed amendment(s): (a) ☑ will not be entered, or (b) ☐ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____
9. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
10. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
11. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

12. ☑ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
13. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
14. ☑ Other: PTO-2323.

STATUS OF CLAIMS

15. The status of the claim(s) is (or will be) as follows:
    Claim(s) allowed: _____.
    Claim(s) objected to: _____.
    Claim(s) rejected: 1-9 and 12-14.
    Claim(s) withdrawn from consideration: _____.

/SULAIMAN NOORISTANY/ Primary Examiner, Art Unit 2415	

Continuation of REQUEST FOR RECONSIDERATION/OTHER 12. The request for reconsideration has been considered but does NOT place the application in condition for allowance because: Response to Arguments
Applicant's arguments filed on 07/22/21 have been fully considered but they are not persuasive.
Applicant Argument:
Regarding first paragraph of 35 U.S.C. 112 rejection, Applicant is suggesting for support to some page Nos. 5, 7, 9 and Figure 2 and Figure 4 of US Non-provisional patent application serial number 11/901,802.

Response to Arguments:
With respect to the above argument, Examiner would like to draw attention that the US Non-provisional patent application serial number 11/901,802 or any other cross reference related Applications does not support the limitation "use HTTP to send user preference to the user data publishing website over the cellular data network" as recited in claim 7 & 14. Thus, the Examiner maintains the rejection.

Applicant Argument: 1
Prior art failed to teach 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, 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.

Response to Arguments:
In addition, the Examiner would like to draw attention to (fig. 1, [0013]) of Hunter, for example: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween.... The Examiner further would like to draw attention to ([0017-0027, 0036-0037-0038]) of Hunter, for example - After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038] (herein it's considered same as 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, 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).

Applicant Argument: 2
Prior art failed to teach "wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data"

Response to Arguments:
In addition, the Examiner would like to draw attention to (fig. 8, 9A-9D, [0099-0110]) of Pietruszka, for example: As shown in FIG. 8, user interface 814 is also coupled to processor 810. User interface 814 facilitates the exchange of information with a user. FIG. 8 shows that user interface 814 includes a user input portion 820 and a user output portion 822. User input portion 820 may include one or more components that allow a user to input information. Examples of such components include keypads, touch screens, and microphones. User output portion 822 allows a user to receive information from the device. Thus, user output portion 822 may include various components, such as a display, and one or more audio speakers. Exemplary displays include liquid crystal displays (LCDs), and video displays. The user interface 814 can allow a user to perform various tasks including among other things those tasks associated with the security or protection embodiments described herein, including for example setting or

LifeScan, Inc. Ex. 1006
Page 72 of 353
IPR2025-00102

changing of the operational state (e.g., Locked, Unlocked, Selective, etc.) of the device or other remote devices, entering or changing passwords, and so forth……(herein it's considered same as wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data).

Applicant Argument: 3-5
Prior art failed to teach pairing short range wireless or away from permanent paired short-range wireless connection and cryptographic pairing between devices
Response to Arguments:
With respect to the above argument, Examiner would like to draw attention to that it is the claims that define the claimed invention, and it is claims, not specifications that are anticipated or unpatentable. Constant v. Advanced Micro-Devices Inc., 7 USPQ2d 1064.
In addition, the Examiner would like to draw attention to (fig. 1, [0017-0027, 0036-0037]) of Hunter, for example: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10 to establish a data link between the two units. Alternatively, the camera 10 may periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10.
The Examiner further would like to draw attention to ([0037]) of Hunter, for example: a device that wishes to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt data exchanged over a wireless medium as an added security. The encryption can however be turned off and passkeys can be stored on the device's file system rather than the Bluetooth component or chip itself. Since the Bluetooth address can be permanent, a pairing can be preserved even if the Bluetooth name is changed. Either device in a pairing relationship may delete the pairing between the devices. Devices may require pairing or may prompt the user before it allows a remote device to utilize any or all or some of its services (herein it's considered same as paired short-range wireless connection and cryptographic pairing between devices).
Furthermore, the Examiner would like to draw attention to (fig. 1-9) of Pietruszka, for example: Accordingly , FIG. 1 is a diagram of an exemplary operational environment 100. This environment includes one or more wireless communications devices (WCDs), such as WCD 110 and WCD 120, which can establish trusted relationships with each other or with other devices to facilitate subsequent wireless communications between the trusted devices and/or set or change an operational state of device pertaining to the handling of the establishment of trusted relationships with other devices. As shown, WCD 110 includes operational state(s) which control its ability to establish a trusted relationship with other devices, such as WCD 120 or other devices. As shown by reference to numeral 112, the operational states may include a locked state to prevent (or prohibit) establishing of a trusted relationship with a remote device or an unlocked state to allow establishing of a trusted relationship with a remote device. Other operational states may also be included such as a selective state, e.g., selective locked or selective unlocked, in which a particular subset or type of device, which may be defined by some discernable category or characteristic (e.g., manufacturer, type of device, and so forth), may be allowed or prevented from establishing a trusted relationship. The operational states may be implemented through a security application resident in one or both of WCD 110, 120 (herein it's considered same as paired short-range wireless connection and cryptographic pairing between devices).

Applicant Argument: 6
Prior art failed to teach receiving or making Phone call trigger even vs NO such Phone call trigger event.

Response to Arguments:
In addition, the Examiner would like to draw attention to (fig. 1, [0013]) of Hunter, for example: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween (herein it's considered same as sending a signal to the cryptographically authenticated short-range wireless enabled cellular

LifeScan, Inc. Ex. 1006
Page 73 of 353
IPR2025-00102

phone corresponding to the acquired new-data).

Applicant Argument: 7
Prior art failed to teach setting based control of cryptographic pairing between devices in NOT relevant in application's scenario
Response to Arguments:
The Examiner further would like to draw attention to ([0017-0027, 0036-0037-0038]) of Hunter, for example - After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038].
In addition, the Examiner would like to draw attention to (fig. 1-9, [0024-0025]) of Pietruszka, for example: Accordingly, FIG. 1 is a diagram of an exemplary operational environment 100. This environment includes one or more wireless communications devices (WCDs), such as WCD 110 and WCD 120, which can establish trusted relationships with each other or with other devices to facilitate subsequent wireless communications between the trusted devices and/or set or change an operational state of device pertaining to the handling of the establishment of trusted relationships with other devices. As shown, WCD 110 includes operational state(s) which control its ability to establish a trusted relationship with other devices, such as WCD 120 or other devices. As shown by reference to numeral 112, the operational states may include a locked state to prevent (or prohibit) establishing of a trusted relationship with a remote device or an unlocked state to allow establishing of a trusted relationship with a remote device. Other operational states may also be included such as a selective state, e.g., selective locked or selective unlocked, in which a particular subset or type of device, which may be defined by some discernable category or characteristic (e.g., manufacturer, type of device, and so forth), may be allowed or prevented from establishing a trusted relationship. The operational states may be implemented through a security application resident in one or both of WCD 110, 120 (herein it's considered same as cryptographically authenticated short-range wireless that is based control of cryptographic pairing between devices in relevant in application's scenario).

Applicant Argument: 8-9
Prior art failed to teach Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data.

Response to Arguments:
In addition, the Examiner would like to draw attention to (fig. 1, [0013]) of Hunter, for example: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween (herein it's considered same as Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data).
In addition, the Examiner would like to draw attention to (fig. 1, [0017-0027, 0036-0037]) of Hunter, for example: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10 to establish a data link between the two units. Alternatively, the camera 10 may periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10.
The Examiner further would like to draw attention to ([0037]) of Hunter, for example: a device that wishes to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt data exchanged over a wireless medium as an added security. The encryption can however be turned off and passkeys can be stored on the device's file system rather

LifeScan, Inc. Ex. 1006
Page 74 of 353
IPR2025-00102

than the Bluetooth component or chip itself. Since the Bluetooth address can be permanent, a pairing can be preserved even if the Bluetooth name is changed. Either device in a pairing relationship may delete the pairing between the devices. Devices may require pairing or may prompt the user before it allows a remote device to utilize any or all or some of its services…
The Examiner further would like to draw attention to ([0017-0027, 0036-0037-0038]) of Hunter, for example - After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone (herein it's considered same as Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data).

Applicant Argument: 10
Prior art failed to teach use HTTP to transfer new-data and a user authentication credential to website

Response to Arguments:
In addition, the Examiner would like to draw attention to (fig. 1, [0009, 0031, 0041]) of Hunter, for example: it is known for mobile telephones to support data instead of or as well as voice calls, in which case the present invention can be taken to relate also to the establishment of a data link or the initiation of data transmission as a result of use of a telephone to access a data service, e.g. an internet page such as a photo website or a photo printing service (herein it's considered same as use HTTP to transfer new-data and a user authentication credential to website).

Applicant Argument: 11
Prior art failed to teach the Claim 12 Polling limitation of: Short-range wireless enabled cellular phone sends a polling request to a short-range wireless enabled data capture device, over an established paired short-range wireless connection, to detect new-data for transfer from the short-range wireless enabled data capture device to the paired and cryptographically authenticated short-range wireless enabled cellular phone
Response to Arguments:
The Examiner would like to draw attention to (fig. 1, [0013]) of Hunter, for example: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween..
The Examiner further would like to draw attention to ([0017-0027, 0036-0037-0038]) of Hunter, for example - After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038] (herein it's considered same as the Claim 12 Polling limitation of…)
Thus, for the above reason, the prior art meet the claim limitation.

The examiner stresses that the claims are too broad and require detail or specialization of the steps as recited in the claims. Alone and as claimed, the limitations are too open.

Examiner has cited particular portions of the references as applied to each claim limitation for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Regarding all other arguments presented by applicant, the arguments are substantially the same as those

LifeScan, Inc. Ex. 1006
Page 75 of 353
IPR2025-00102

which have already been addressed above and in the interest of brevity; the Examiner directs the applicant to those responses above.

LifeScan, Inc. Ex. 1006
Page 76 of 353
IPR2025-00102

AFCP 2.0 Decision

Application No.	Applicant(s)	
16/532,507	Singh et al.	
Examiner	**Art Unit**	**AIA (FITF) Status**
SULAIMAN NOORISTANY	2415	No

This is in response to the After Final Consideration Pilot request filed 22 July 2021.

1. **Improper Request** – The AFCP 2.0 request is improper for the following reason(s) and the after final amendment submitted with the request will be treated under pre-pilot procedure.

   ☐ An AFCP 2.0 request form PTO/SB/434 (or equivalent document) was not submitted.

   ☐ A non-broadening amendment to at least one independent claim was not submitted.

   ☐ The request is not the first proper AFCP 2.0 request submitted in response to the most recent final rejection.

   ☐ Other: _____

2. **Proper Request**

   A. After final amendment submitted with the request will not be treated under AFCP 2.0.
   The after final amendment cannot be reviewed and a search conducted within the guidelines of the pilot program.

   ☑ The after final amendment will be treated under pre-pilot procedure.

   B. Updated search and/or completed additional consideration.
   The examiner performed an updated search and/or completed additional consideration of the after final amendment within the time authorized for the pilot program. The result(s) of the updated search and/or completed additional consideration are:

   ☐ 1. All of the rejections in the most recent final Office action are overcome and a Notice of Allowance is issued herewith.

   ☐ 2. The after final amendment would not overcome all of the rejections in the most recent final Office action . See attached interview summary for further details.

   ☐ 3. The after final amendment was reviewed, and it raises a new issue(s). See attached interview summary for further details.

   ☐ 4. The after final amendment raises new issues, but would overcome all of the rejections in the most recent final Office action. A decision on determining allowability could not be made within the guidelines of the pilot. See attached interview summary for further details, including any newly discovered prior art.

   ☐ 5. Other: _____

   Examiner Note: Please attach an interview summary when necessary as described above.

DO NOT ENTER: /S.N/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re. application of:
Gurvinder Singh
Application No.: 16/532,507 Examiner: Nooristany, Sulaiman
Filed: 08/06/2019 Art Unit: 2415
Applicant: Cellspinsoft Inc. Atty. Docket no.: CellSpin_04Con17_US
Title: Automatic Multimedia Upload
For Publishing Data And Multimedia Content

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Response under "After Final Consideration Pilot Program 2.0"

Examiner Nooristany:

In response to the final office action mailed June 08, 2021, please amend the above-referenced application as follows:

Amendments to the claims are listed on page 2 of this response.

Remarks begin on page 11 of this response.

LifeScan, Inc. Ex. 1006
Page 78 of 353
IPR2025-00102

Doc Code: A.NE.AFCP
Document Description: After Final Consideration Pilot Program Request

PTO/SB/434 (12-20)

CERTIFICATION AND REQUEST FOR CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0

Practitioner Docket No.:	Application No.:	Filing Date:
CellSpin_04Con17_US	16/532,507	08/06/2019
First Named Inventor:	**Title:**	
Gurvinder Singh	Automatic Multimedia Upload For Publishing Data And Multimedia Content	

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS CONSIDERATION UNDER THE AFTER FINAL CONSIDERATION PILOT PROGRAM 2.0 (AFCP 2.0) OF THE ACCOMPANYING RESPONSE UNDER 37 CFR 1.116.

1. The above-identified application is (i) an original utility, plant, or design nonprovisional application filed under 35 U.S.C. 111(a) [a continuing application (*e.g.*, a continuation or divisional application) is filed under 35 U.S.C. 111(a) and is eligible under (i)], or (ii) an international application that has entered the national stage in compliance with 35 U.S.C. 371(c).
2. The above-identified application contains an outstanding final rejection.
3. Submitted herewith is a response under 37 CFR 1.116 to the outstanding final rejection. The response includes an amendment to at least one independent claim, and the amendment does not broaden the scope of the independent claim in any aspect.
4. This certification and request for consideration under AFCP 2.0 is the only AFCP 2.0 certification and request filed in response to the outstanding final rejection.
5. Applicant is willing and available to participate in any interview requested by the examiner concerning the present response.
6. This certification and request is being filed electronically using the Office's electronic filing system (EFS-Web).
7. Any fees that would be necessary consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, extension of time fees, are being concurrently filed herewith. [There is no additional fee required to request consideration under AFCP 2.0.]
8. By filing this certification and request, applicant acknowledges the following:
   - Reissue applications and reexamination proceedings are not eligible to participate in AFCP 2.0.
   - The examiner will verify that the AFCP 2.0 submission is compliant, *i.e.*, that the requirements of the program have been met (see items 1 to 7 above). For compliant submissions:
     - The examiner will review the response under 37 CFR 1.116 to determine if additional search and/or consideration (i) is necessitated by the amendment and (ii) could be completed within the time allotted under AFCP 2.0. If additional search and/or consideration is required but cannot be completed within the allotted time, the examiner will process the submission consistent with current practice concerning responses after final rejection under 37 CFR 1.116, *e.g.*, by mailing an advisory action.
     - If the examiner determines that the amendment does not necessitate additional search and/or consideration, or if the examiner determines that additional search and/or consideration is required and could be completed within the allotted time, then the examiner will consider whether the amendment places the application in condition for allowance (after completing the additional search and/or consideration, if required). If the examiner determines that the amendment does not place the application in condition for allowance, then the examiner will contact the applicant and request an interview.
       - The interview will be conducted by the examiner, and if the examiner does not have negotiation authority, a primary examiner and/or supervisory patent examiner will also participate.
       - If the applicant declines the interview, or if the interview cannot be scheduled within ten (10) calendar days from the date that the examiner first contacts the applicant, then the examiner will proceed consistent with current practice concerning responses after final rejection under 37 CFR 1.116.

Signature	Date	Practitioner Registration No.
/Ash Tankha/	07/22/2021	33802
Name (Print/Typed)	**Telephone Number**	
Ashok Tankha	856-266-5145	

Note: *This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.*

☐ * Total of _____ forms are submitted.

LifeScan, Inc. Ex. 1006
Page 79 of 353
IPR2025-00102

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

LifeScan, Inc. Ex. 1006
Page 80 of 353
IPR2025-00102

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re. application of:
Gurvinder Singh
Application No.: 16/532,507 Examiner: Nooristany, Sulaiman
Filed: 08/06/2019 Art Unit: 2415
Applicant: Cellspinsoft Inc. Atty. Docket no.: CellSpin_04Con17_US
Title: Automatic Multimedia Upload
For Publishing Data And Multimedia Content

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Response under "After Final Consideration Pilot Program 2.0"

Examiner Nooristany:

In response to the final office action mailed June 08, 2021, please amend the above-referenced application as follows:

Amendments to the claims are listed on page 2 of this response.

Remarks begin on page 11 of this response.

Amendments to the claims

Claim 1 (previously presented): A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device;

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, wherein the event notification corresponds to the acquired new-data and comprises sending a signal to the cryptographically authenticated short-

LifeScan, Inc. Ex. 1006
Page 82 of 353
IPR2025-00102

range wireless enabled cellular phone, 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, wherein a 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, wherein the 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, 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 and the user authentication credential to a user data publishing website over a cellular data network, and wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data.

Claim 2 (previously presented): 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.

Claim 3 (previously presented): The short-range wireless enabled data capture device of claim 1, wherein the user authentication credential sent by the 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.

Claim 4 (previously presented): A system, comprising:

a short-range wireless enabled data capture device, comprising:

LifeScan, Inc. Ex. 1006
Page 83 of 353
IPR2025-00102

a first memory device;

a first processor coupled to the first memory device;

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;

a data capture circuitry;

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;

said first processor further configured to store the new-data in the first memory device; and

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;

4

LifeScan, Inc. Ex. 1006
Page 84 of 353
IPR2025-00102

said short-range wireless enabled cellular phone, comprising:

a second memory device;

a second processor coupled to the second memory device;

a cellular network communication device configured to connect to the internet via a cellular data network;

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;

a 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, wherein the mobile client application for the short-range wireless enabled cellular phone is configured to process the event notification;

receive the new-data from the short-range wireless enabled data capture device;

store the received new-data in the second memory device;

store a user authentication credential in the second memory device;

5

LifeScan, Inc. Ex. 1006
Page 85 of 353
IPR2025-00102

use HTTP to upload the received new-data and the user authentication credential to a user data publishing website over the cellular data network; and

provide a touch based graphical user interface for the received new-data.

Claim 5 (previously presented): 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.

Claim 6 (previously presented): The system of claim 4, wherein the user authentication credential is for a user of the user data publishing website.

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

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

Claim 8 (previously presented): A short-range wireless enabled cellular phone, comprising:

a memory device;

a processor coupled to the memory device;

a cellular network communication device configured to connect to internet via a cellular data network;

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;

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:

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;

receive the event notification and the new-data from the short-range wireless enabled data capture device;

process the event notification and store the received new-data in the memory device;

store a user authentication credential in the memory device;

LifeScan, Inc. Ex. 1006
Page 87 of 353
IPR2025-00102

use HTTP to upload the received new-data and the user authentication credential to a user data publishing web service over the cellular data network; and

provide a touch based graphical user interface for the received new-data.

Claim 9 (previously presented): The short-range wireless enabled cellular phone of claim 8, 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.

Claims 10-11 (cancelled).

Claim 12 (previously presented): A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device of the short-range wireless enabled data capture device;

said processor further configured to listen to a polling request from a 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, wherein the 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 mobile client application on the short-range wireless enabled cellular phone, over the established paired short-range wireless connection;

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 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 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 mobile client application for the short-range wireless enabled cellular phone stores a user authentication credential in the memory device of the

LifeScan, Inc. Ex. 1006
Page 89 of 353
IPR2025-00102

short-range wireless enabled cellular phone, wherein the mobile client application on the short-range wireless enabled cellular phone is further 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, and wherein the mobile client application on the short-range wireless enabled cellular phone provides a touch based GUI for the received new-data.

Claim 13 (previously presented): The short-range wireless enabled data capture device of claim 12, 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.

Claim 14 (previously presented): The short-range wireless enabled data capture device of claim 12, wherein the mobile client application for the short-range wireless enabled cellular phone uses HTTP to send user preferences to the user data publishing web service over the cellular data network, wherein the user preferences comprise global positioning system information.

LifeScan, Inc. Ex. 1006
Page 90 of 353
IPR2025-00102

Remarks

The pending claims

Claims 1-9 and 12-14 are currently pending. Reconsideration and allowance of the pending claims is respectfully requested.

Summary of the Office Action

Summary of the Office Action

Summary of examiner interview on 07 May 2021

Applicant thanks the examiner for providing a telephonic interview on 07 May 2021.

Claim Rejections - 35 USC § 112

Claims 7, 14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

Specification Objection

The disclosure is objected to because of the following informalities: Examiner has reviewed the specification of this application under examination and could not find support for the additional limitations as claimed "use HTTP to send global positioning system information to the user data publishing website over the cellular data network". Appropriate correction is required.

Claim Rejections - 35 USC § 112

Claims 7, 14 are rejected under 112, second paragraph as being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention.

Claim Rejections 35 U.S.C. 103

Claim 1-6, 8-9, 12-13 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778.

Claim 7 & 14 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778 further in view of Risbood US 20070111748

Support for claim limitations

Support for the limitation: "*use HTTP to send user preferences to the user data publishing website over the cellular data network, wherein the user preferences comprise global positioning system information*" in claim 7 is found in:

(a) Point No. 2 of "CROSS REFERENCE TO RELATED APPLICATIONS" in the originally filed application, which states as follows: "*The following patent application is* ***incorporated herein in its entirety****: US Non-provisional patent application serial number 11/901,802, titled "Online Publishing of Multimedia Content", filed on September 19, 2007 in the United States Patent and Trademark Office." USPTO Publication No. 2008/0103906 A1 is the published application of US Non-provisional patent application serial number 11/901,802. US Non-provisional patent application serial number 11/901,802 is attached to the response to previously submitted response to non-final office action as Exhibit A and USPTO Publication No. 2008/0103906 A1 is attached to the previously submitted response to non-final office action as Exhibit B; see also link:*

LifeScan, Inc. Ex. 1006
Page 92 of 353
IPR2025-00102

https://patentimages.storage.googleapis.com/1f/06/a0/32f9a69fbef2a6/US20080103906A.pdf."

(b) Paragraph [0023] of Exhibit B, which states: "*The multimedia object is published 108 by the front end service 204b according to the user preferences on one or more publication virtual spaces 205 via the network 203.* ***The user preferences*** *may comprise* ***authentication credentials****, transaction identification,* ***a list of publication virtual spaces 205****,* ***global positioning system geographical codes***."

(c) Paragraph [0024] of Exhibit B, which states: "*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***."

(d) Paragraph [0028] of Exhibit B, which states: "*The preferences set by the user 201 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.* ***These user preferences are transferred to the publishing service 204."***

(e) Paragraph [0047] of Exhibit B, which states: "***The user 201 transfers*** *the* ***multimedia*** *object for publishing to a publication space selected by the user 201.* ***Additional information such as*** *the list of* ***the user preferences of the publication virtual spaces 205****,* ***authentication identification****, user preferences, default settings, manually entered* ***geographical codes****, and auction identifiers for eBay® and other shopping websites are selected 407 and* ***transferred along with the user created multimedia content to the publishing service 204***."

(f) Paragraph [0018] of Exhibit B, which states: "*The client application 202 communicates the user publishing information including the* ***user preferences of***

LifeScan, Inc. Ex. 1006
Page 93 of 353
IPR2025-00102

the publication virtual spaces 205 *to the front end service 204b*", Paragraph [0023] of Exhibit B, which states: "*The* ***user preferences*** ***may comprise authentication credentials****, transaction identification,* ***a list of publication virtual spaces 205****,* ***global positioning system geographical codes***", Paragraph [0025] of Exhibit B, which states: "*The client application 202 enables the user 201 of the mobile device to record and transfer the user created multimedia content to the publishing service 204*", ***Paragraph [0061] of*** *Exhibit B, which states: "****The transport protocol that is used*** *between the client application 202 and the publishing service 204 may be* ***hypertext transfer protocol (HTTP)***".

The office action states: "**Claims 1-9, 12-14 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claims of parent Application(s) No. 15659637, 14578202, 14503401, 14273546, 14172913, 13740214, 12333303 and co-pending Application No. 11901802. Although the claims at issue are identical, they are not patentably distinct from each other because they are same variants of each other.**"

In response to the above rejection, applicant submits terminal disclaimers for patent application Nos. 15659637, 14578202, 14503401, 14273546, 14172913, 13740214, 12333303 and co-pending Application No. 11901802 as suggested in the office action. Applicant therefore respectfully requests that the double patenting rejection be reconsidered and withdrawn.

The office action further states: "**Claims 7, 14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The applicant fails to sufficiently point out or describe use of HTTP to send global positioning system information to the user data publishing website over the cellular data network.**"

In response to the above rejection, applicant submits that the recitation: "*use HTTP to send user preferences to the user data publishing website over the cellular data*

LifeScan, Inc. Ex. 1006
Page 94 of 353
IPR2025-00102

network, wherein the user preferences comprise global positioning system information" in amended claim 7 is supported in the following paragraphs of Exhibit B:

(a) Paragraph [0018] of Exhibit B, which states: "The client application 202 communicates the user publishing information including the **user preferences of the publication virtual spaces 205** to the front end service 204b".

(b) **Paragraph [0023] of Exhibit B**, which states: "The **user preferences may comprise authentication credentials**, transaction identification, **a list of publication virtual spaces 205**, **global positioning system geographical codes**",

(c) Paragraph [0025] of Exhibit B, which states: "The client application 202 enables the user 201 of the mobile device to record and transfer the user created multimedia content to the publishing service 204".

(d) Paragraph [0061] of Exhibit B, which states: "The **transport protocol that is used** between the client application 202 and the publishing service 204 may be **hypertext transfer protocol (HTTP)".**

Applicant therefore respectfully submits that the following recitation in amended claim 7 is fully supported in Exhibit B:

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

Applicant therefore respectfully requests that the rejection of claim 7 under 35 U.S.C. 112, first paragraph be reconsidered and withdrawn.

LifeScan, Inc. Ex. 1006
Page 95 of 353
IPR2025-00102

Amended claim 14 is analogous to amended claim 7 and recites the same limitation as in amended claim 7. Applicant therefore respectfully requests that the rejection of claim 14 under 35 U.S.C. 112, first paragraph be reconsidered and withdrawn.

The office action further states: "**The disclosure is objected to because of the following informalities: Examiner has reviewed the specification of this application under examination and could not find support for the additional limitations as claimed "use HTTP to send global positioning system information to the user data publishing website over the cellular data network". Appropriate correction is required.**"

In response to the above objection, applicant submits that "*use HTTP to send user preferences to the user data publishing website over the cellular data network, wherein the user preferences comprise global positioning system information*" is supported in the following paragraphs of Exhibit B:

(a) Paragraph [0018] of Exhibit B, which states: "The client application 202 communicates the user publishing information including the **user preferences of the publication virtual spaces 205** to the front end service 204b".

(b) Paragraph [0023] of Exhibit B, which states: "The **user preferences** may comprise **authentication credentials**, transaction identification, **a list of publication virtual spaces 205**, **global positioning system geographical codes**".

(c) Paragraph [0025] of Exhibit B, which states: "The client application 202 enables the user 201 of the mobile device to record and transfer the user created multimedia content to the publishing service 204".

LifeScan, Inc. Ex. 1006
Page 96 of 353
IPR2025-00102

(d) Paragraph [0061] of Exhibit B, which states: "The **transport protocol that is used** between the client application 202 and the publishing service 204 may be **hypertext transfer protocol (HTTP)**".

Applicant therefore respectfully submits that the objection to the specification be reconsidered and withdrawn.

The office action further states: "**Claims 7, 14 are rejected under 112, second paragraphs being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention. In claim 7, the terms "use HTTP to send global positioning system information to the user data publishing website over the cellular data network" are not clear what these are in reference to.**"

In response to the above rejection, applicant submits that "*use HTTP to send user preferences to the user data publishing website over the cellular data network, wherein the user preferences comprise global positioning system information*" is fully supported in the following paragraphs of Exhibit B:

(a) Paragraph [0018] of Exhibit B, which states: "The client application 202 communicates the user publishing information including the **user preferences of the publication virtual spaces 205** to the front end service 204b".

(b) Paragraph [0023] of Exhibit B, which states: "The **user preferences may comprise authentication credentials**, transaction identification, **a list of publication virtual spaces 205**, **global positioning system geographical codes**".

(c) Paragraph [0025] of Exhibit B, which states: "The client application 202 enables the user 201 of the mobile device to record and transfer the user created multimedia content to the publishing service 204".

LifeScan, Inc. Ex. 1006
Page 97 of 353
IPR2025-00102

(d) Paragraph [0061] of Exhibit B, which states: "The **transport protocol that is used** between the client application 202 and the publishing service 204 may be **hypertext transfer protocol (HTTP)**".

Applicant therefore respectfully requests that the rejection of claim 7 under 35 U.S.C. 112, second paragraph be reconsidered and withdrawn.

Amended claim 14 is analogous to amended claim 7 and recites the same limitation as in amended claim 7. Applicant therefore respectfully requests that the rejection of claim 14 under 35 U.S.C. 112, first paragraph be reconsidered and withdrawn.

The office action further states: "**Claim 1-6, 8-9, 12-13 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778.**"

In response to the above rejection, applicant submits that Hunter, in view of Pietruszka does not teach or suggest all the limitations in claims 1 and 12.

Arguments:

Argument#1:

The office action states that paragraph [0013] of Hunter is teaching the following limitation in claim 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, 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".

Applicant respectfully *disagrees* and submits the following arguments:

Hunter [0013]

[**0013**] In accordance with a fourth aspect of the invention, there is provided method of capturing and communicating images, comprising the steps of: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognising occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween; transferring images between the camera and the communications device over the wireless link; and transferring said images from the communications device on to a data network through a data network interface.

Recognizing ≠ Sending

In fact, it is the opposite of *sending*.



LifeScan, Inc. Ex. 1006
Page 99 of 353
IPR2025-00102

(a) In **Hunter** paragraph [0013], the Camera is ***recognizing*** **a trigger event**. In applicant's claim 1, the Camera is **Sending** an event notification.

(b) Recognizing an event trigger (Hunter) is not same as Sending an event notification in applicant's claim 1.

(c) Recognize is not the same as Sending

(d) In Hunter paragraph [0013], the Camera is recognizing a trigger event sent by the phone and then the camera is acquiring the image.

(e) In applicant's claim 1, the Camera is Sending an event notification, for the image that has already been acquired.

(f) In Hunter paragraph [0013], the "event trigger" is to acquire an image.

(g) In applicant's claim 1, the "event notification" corresponds to the image that has already been acquired.

(h) Receiving an Event trigger to acquire an image is not same as sending an event notification for the image already acquired.

Note: See extract of office action reproduced below and applicant's response:

LifeScan, Inc. Ex. 1006
Page 100 of 353
IPR2025-00102

said first processor further configured to send an event notification **(Hunter: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween [0013])** and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically **(Hunter: transferring images between the camera and the communications device over the wireless link [0013])**, 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 **(Hunter: [0013])**.

- In Hunter [0013] the Camera is **recognizing** a trigger event.
- In our claims the Camera is **Sending** an event notification.
- Recognize an event trigger ≠ Sending an event notification
- Recognize ≠ Sending

- In Hunter [0013] the Camera is **recognizing** a trigger event sent by the phone and then the camera is taking the image.
- In our claims the Camera is **Sending** an event notification, for the image that has *already been taken*.
- In Hunter [0013] the "event trigger" **is to take an image**
- In our case the "event notification" corresponds to the image that has *already been taken*
- Receiving an Event trigger to take an image ≠ sending an event notification for the image already taken.

Argument #2:

Furthermore, the office action states that paragraph [0025] of Hunter and paragraph [0099] of Pietruszka teach the following limitation in claim 1:

> "wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data"

Applicant respectfully *disagrees* and submits the following arguments:

(a) In Hunter paragraph [0025], the touch interface and operation is on the camera device and for the image acquired on/by the camera.

(b) In applicant's claim 1, the touch interface is on the mobile device and is for the image received from the camera.

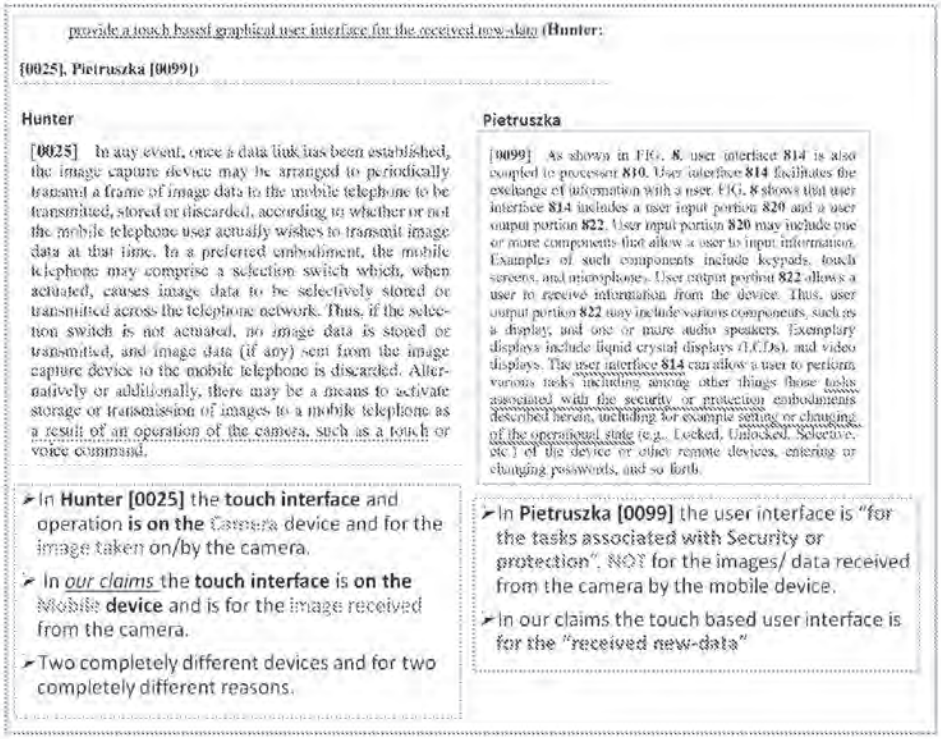
(c) Two completely different devices and for two completely different reasons.

(d) In Pietruszka paragraph [0099], the user interface is "for the tasks associated with Security or protection"; NOT for the images/ data received from the camera by the mobile device'

(e) In applicant's claim 1, the touch based user interface is for the "received new-data".

Note: See extract of office action reproduced below and applicant's response:

LifeScan, Inc. Ex. 1006
Page 102 of 353
IPR2025-00102



Argument #3:

Furthermore, the office action states that paragraph [0037] and FIGS. **9A-9D** of Pietruszka teach the following limitation in claim 1:

> "wherein the 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."

Applicant respectfully *disagrees* and submits the following arguments:

Paragraph [0037] of Pietruszka discloses cryptographically authenticating a short-range wireless device. In contrast, applicant's claim 1 recites storing of website "user"

LifeScan, Inc. Ex. 1006
Page 103 of 353
IPR2025-00102

authentication credentials on the mobile. Furthermore, FIGS. **9A-9D** disclose that the authentication is for the short-range wireless device and NOT for a website user.

Therefore, applicant submits that "*Cryptographic authentication of a wireless device*" in Pietruszka is not same as "*Website user authentication credentials*" as recited in applicant's claim 1.

To illustrate the point with an example, a *Facebook or YouTube website* ***"user authentication credential"*** is completely different from a cryptographic authentication being performed between & by *two devices* such as a camera and a mobile phone.

Note: See extract of office action reproduced below and applicant's response:

> **Pietruszka** further teaches cryptographically authenticating (**Pietruszka: [0037]**); store the user authentication credential in the second memory device (**Pietruszka fig. 9A-9D**) and

> **[0037]** A device that wishes to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt data exchanged over a wireless medium as an added security. The encryption can however be turned off and passkeys can be stored on the device's file system rather than the Bluetooth component or chip itself. Since the Bluetooth address can be permanent, a pairing can be preserved even if the Bluetooth name is changed. Either device in a pairing relationship may delete the pairing between the devices. Devices may require pairing or may prompt the user before it allows a remote device to utilize any or all or some of its services.

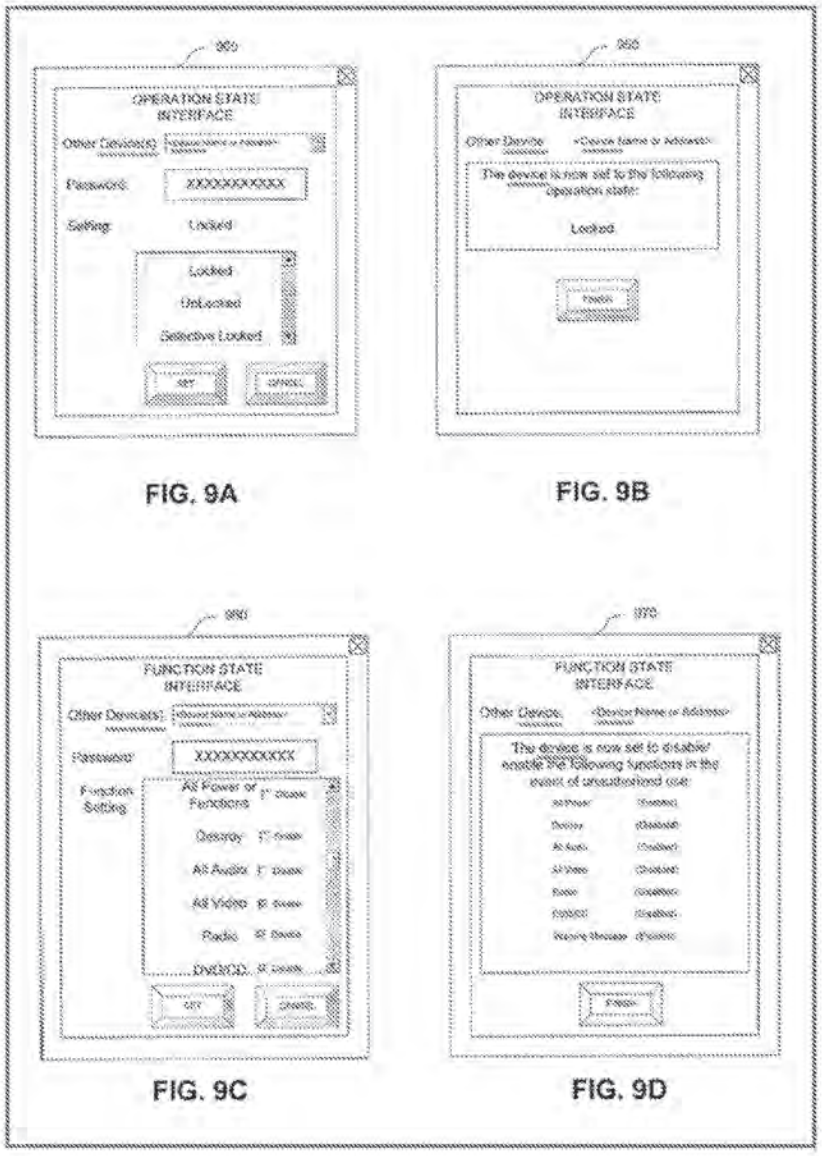


FIG. 9A

FIG. 9B

FIG. 9C

FIG. 9D

LifeScan, Inc. Ex. 1006
Page 105 of 353
IPR2025-00102

- In **Pietruszka [0037] is talking about cryptographically authenticating a short-range wireless device. Our Claim is about storing website "user" authentication credentials on the mobile!**
- In **Pietruszka [Fig 9A – 9D] make it clear that the authentication is for the Device and NOT a website user**

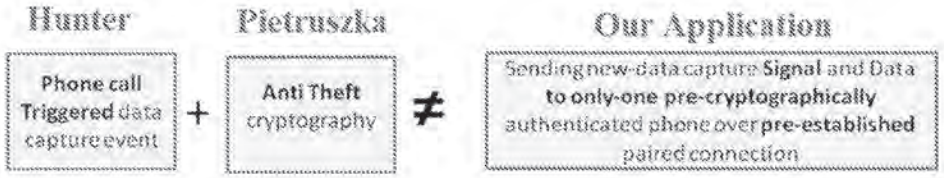
Cryptographic authentication of a wireless device

$\neq$

Website user authentication credentials

Argument #4:

Furthermore, there is no motivation to combine (i) Phone call triggered data capture event of Hunter with (ii) the Anti-Theft Pietruszka teaching.



Argument #5:

Establishment of non-paired connection (Hunter)

VS

Establishment of paired short-range Wireless (Applicant)

The office action on page 7 states that Hunter teaches the step of acquiring new-data 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. Applicant disagrees and presents the following arguments.

Hunter prior art does NOT teach pairing or paired connection. There is NO mention of word pair, pairing, paired in Hunter Specification. Short-range Pairing and Paired wireless connection are terms of short-range wireless technology and have been known and was used in the wireless industry for almost 10 years before the Cellspin patent's priority date of December 2007. Bluetooth wireless standard organization was the first to introduce the term "Bluetooth" at the Blackberry technology consortium in 1998; see Exhibit C, also available at the link: https://web.archive.org/web/20180525083558/https://www.bluetooth.com/about-us/our-history. Furthermore, in 1999, the detailed Bluetooth 1.0 specification with pairing was released; see Exhibit D attached to this response; also available at the link: http://grouper.ieee.org/groups/802/15/Bluetooth/profile_10_b.pdf.

The concept of a paired connection, as established by the Bluetooth Special Interest Group (Bluetooth SIG), became known and adopted by certain other industry organizations creating short-range wireless technology for device connections, such as WiFi Alliance and Zigbee Forum. In the context of short-range wireless connections, the term "pairing" was adopted by the wireless industry almost 10 years before the Cellspin patent's priority date of December 2007. Drawing from short-range wireless industry's understanding of the term "paired connection" / pairing, the broadest reasonable interpretation (BRI) of "paired connection" as understood by POSITA in Dec 2007, i.e. 10 years after the term was introduced in the wireless lexicon is:

> "bidirectional communications link between devices which provides for encrypted data exchange between the devices, and the communication link can be disconnected and reconnected without having to repeat pairing or authentication."

Because short-range "pairing" is a well-understood term in the art, the applicant followed Federal Court's direction that the "patent need not teach, and preferably omits,

LifeScan, Inc. Ex. 1006
Page 107 of 353
IPR2025-00102

what is well known in the art." See McRO, Inc. v. Bandai Namco Games Am. Inc., 959 F.3d 1091, 1102 (Fed. Cir. 2020). In conformance with this guidance, the applicant cited a version of "pairing" at least 50 times without explicitly defining it. Additionally, while not explicitly defining "pairing," the applicant provided guidance to a POSITA that short-range "pairing" should conform to Bluetooth's conception of the term, which was later adopted when ZigBee and WiFi adopted pairing, making it the only definition applicable to short-range paired wireless connections whether or not a Bluetooth Connection.

Argument #6:

Receiving or making Phone call trigger event (Hunter)

VS

NO such Phone call trigger event (Applicant)

The office action on page 6 states that Hunter teaches the step of acquiring new-data 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. Applicant disagrees and presents the following arguments.

The sequence of events in Hunter is as follows:

(i) Mobile device generates a trigger event or signal in response to a phone call received by the mobile device or a phone call made by the mobile device.

(ii) Send the trigger event or signal from the mobile device to the data capture device.

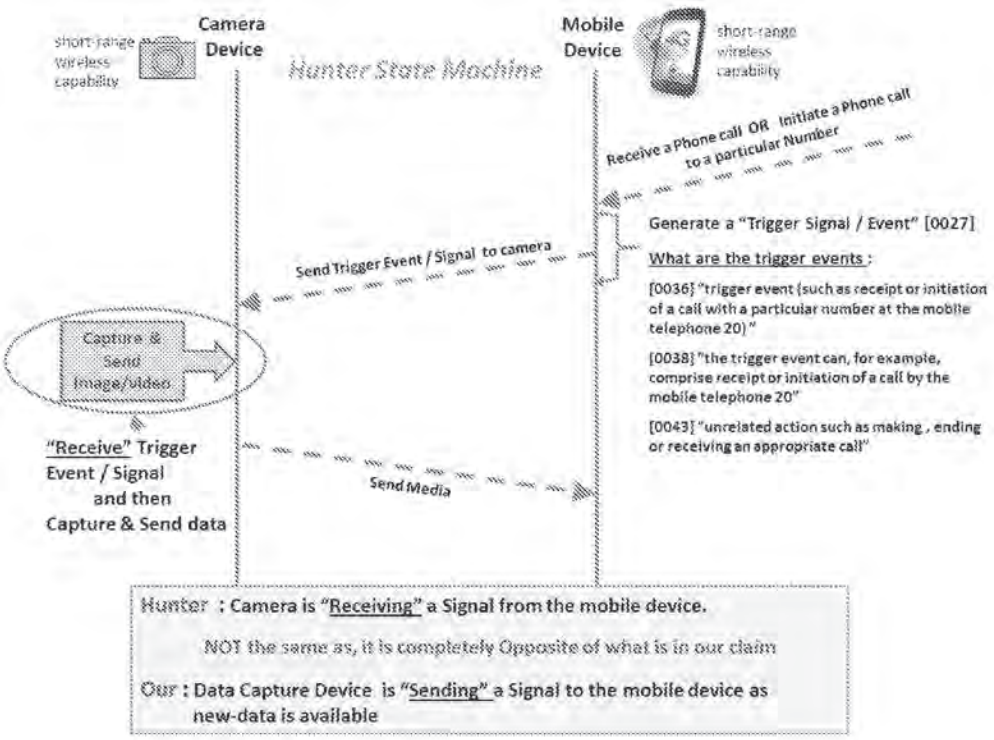
(iii) Only after receipt of the trigger event or signal from the mobile device, the data capture device acquires new-data and transmits the same to the mobile device for onward transfer to a website or web service.

Firstly, in Hunter, there is NO pairing of the mobile device by the data capture device. Next, there is NO cryptographic authentication of the mobile device by the data capture device. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be sent to the data capture device.

Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where a data capture device acquires new-data after a short-range paired wireless connection is established with a cellular phone (without any phone call trigger event from the cellular phone to the data capture device).

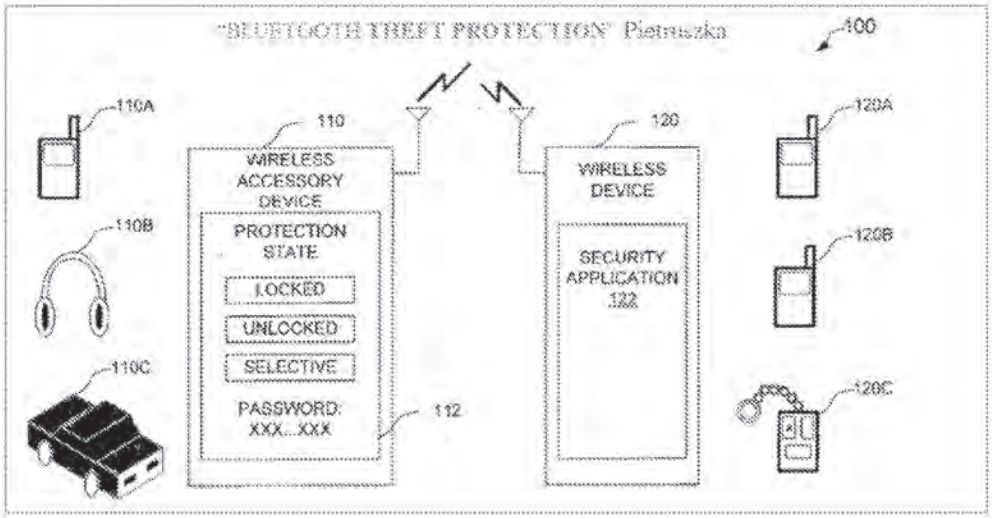
Next, in Hunter, the phone call trigger event is sent from the mobile device to the data capture device. This is in direct contrast to applicant's disclosure, where, after acquiring the new-data, the data capture device sends a notification signal to the mobile device informing the mobile device that it has acquired the new-data.

LifeScan, Inc. Ex. 1006
Page 109 of 353
IPR2025-00102



Argument #7:

Anti-Theft Pietruszka Setting based control of cryptographic pairing between devices is NOT relevant in applicant's scenario



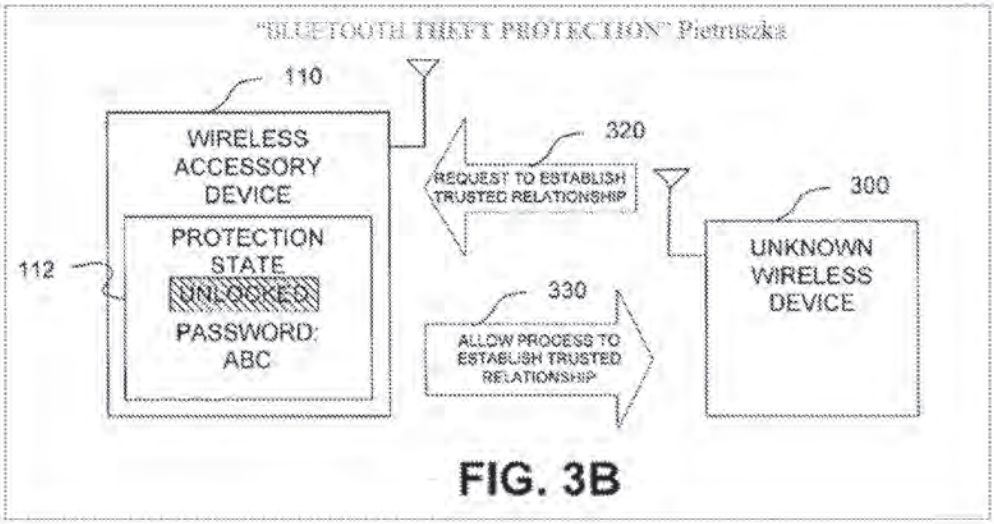


FIG. 3B

Pietruszka ("BLUETOOTH THEFT PROTECTION") discloses, inter alia, the following:

(a) User pre-selects whether or not a wireless communications device is allowed to establish a cryptographic pairing with a remote device.

(b) Control whether the wireless communications device is able to establish a cryptographic pairing with a remote device according to the pre-set operational state; see Pietruszka claim 1, and Paragraph [0005].

Pietruszka teaches mainly a setting-based control of cryptographic pairing between devices and it is not applicable in applicant's scenario. Applicant is NOT using a setting-based control for cryptographic pairing between devices.

Applicant is not implementing any Anti-theft technology. Applicant is not interested in a car or a key fob, or someone else hacking the car to steal it or the car accessories.

Pietruszka teaches mainly an Anti-theft technology and is not applicable in applicant's scenario. Applicant is NOT using pre-set operational state based cryptographic pairing for Anti-Theft purposes for car or car accessories.

Furthermore, in Pietruszka, car or a key fob is "NOT a data capture device" and does not send any data through the mobile phone to the internet.

In Pietruszka there is NO data capture device. Car or a key fob device described in Pietruszka is used as a theft control device. The Car or a key fob device is NOT capturing any data for transfer through the mobile device.

Furthermore, in Pietruszka, NO new-data is acquired for sending to the mobile phone after establishing the short-range paired wireless connection. Pietruszka's invention is all about the theft protection based on pre-set operational state of the device in its proximity.

Furthermore, there is NO Motivation to combine an anti-theft Pietruszka with Hunter to capture data and send data to a website using a cellphone.

LifeScan, Inc. Ex. 1006
Page 112 of 353
IPR2025-00102

In view of above arguments 1-7, applicant submits that Hunter, in view of Pietruszka does not teach or suggest the following limitations in claim 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, 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;"

> "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;"

Argument #8:

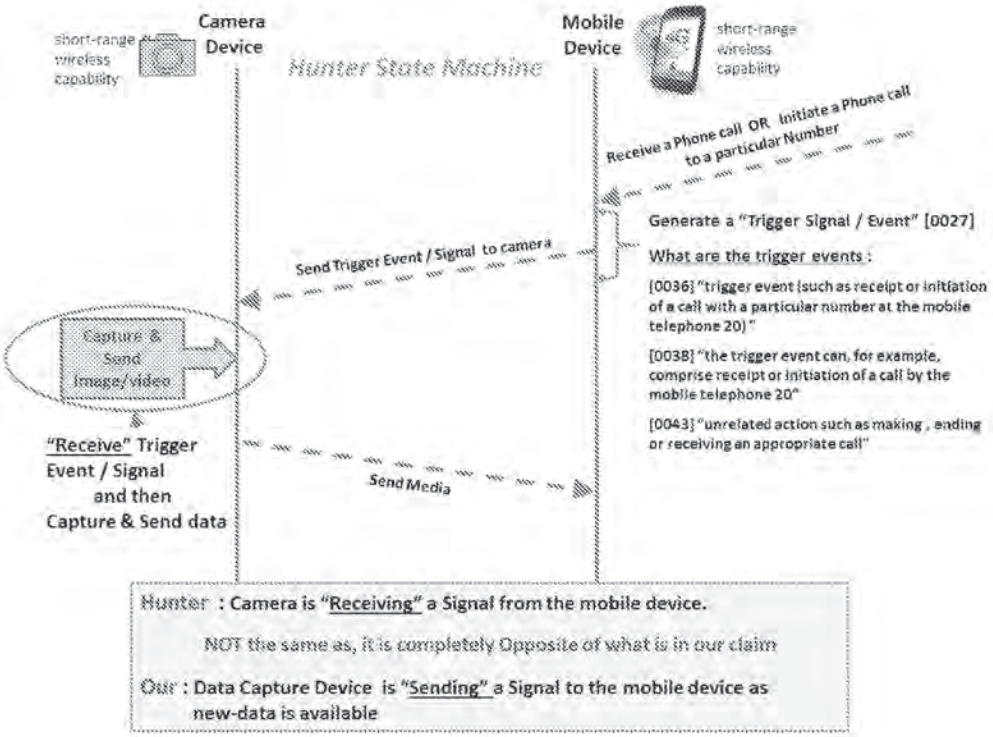
> **Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data.**

In claim 1, applicant discloses that after establishing the paired short-range wireless connection between the data capture device and the cryptographically authenticated short-range wireless enabled cellular phone, and after acquiring new-data, the short-range wireless enabled data capture device sends the event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone.

The office action on page 7 states that paragraph [0013] of Hunter teaches: "Sending an event notification to a cryptographically authenticated Bluetooth enabled cellular phone". Applicant disagrees and presents the following arguments.

Paragraph [0013] of Hunter states as follows: "programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween; transferring images between the camera and the communications device over the wireless link; and transferring said images from the communications device on to a data network through a data network interface."

Hunter state machine is again reproduced below to explain paragraph [0013]:



LifeScan, Inc. Ex. 1006
Page 114 of 353
IPR2025-00102

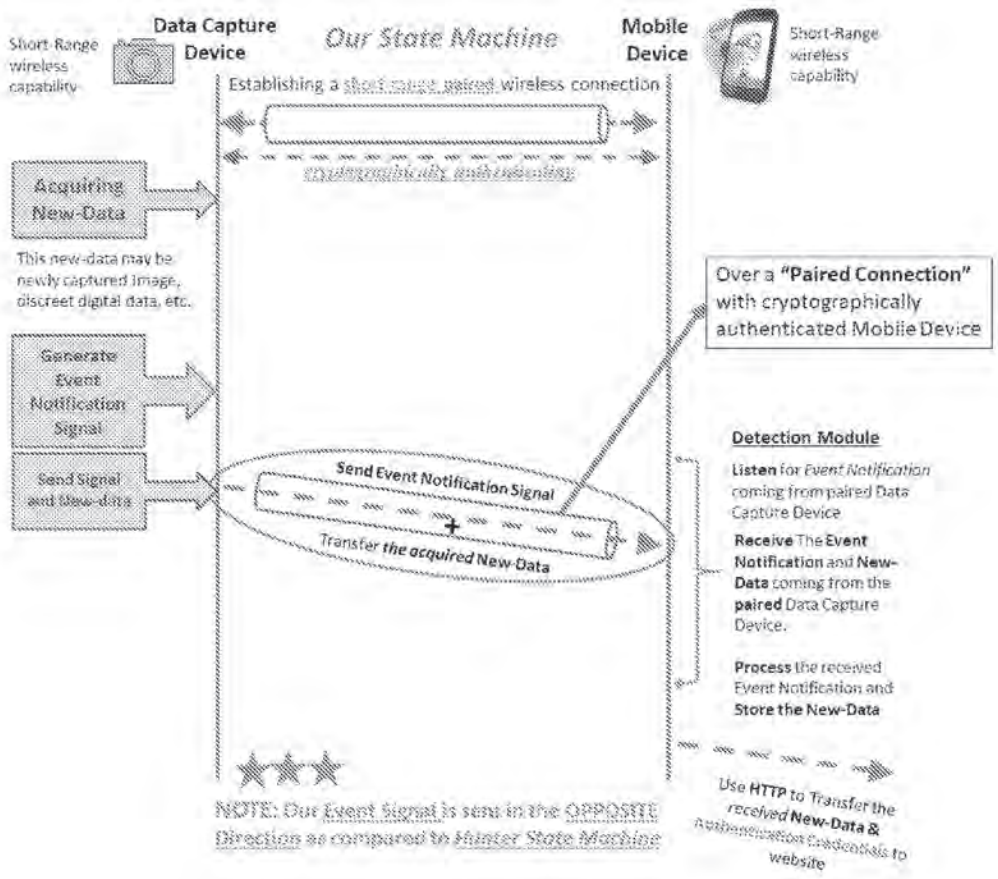
Firstly, in Hunter, there is NO cryptographic authentication of the mobile device by the data capture device before the signal is sent or the data is sent. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be sent to the data capture device.

Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. **This is in direct contrast** to applicant's disclosure where a data capture device acquires new-data after a short-range paired wireless connection is established with a cellular phone (without any phone call trigger event from the cellular phone to the data capture device).

Next, in Hunter, the phone call trigger event is sent from the mobile device to the data capture device. **Event Signal is sent in the opposite direction when compared to the applicants claims.** Direction of event signal is in direct contrast to applicant's disclosure, where, after acquiring the new-data, the data capture device sends a notification signal to the mobile device informing the mobile device that it has acquired the new-data.

In contrast, applicant's state machine is shown below.

LifeScan, Inc. Ex. 1006
Page 115 of 353
IPR2025-00102



Therefore, it is clear that the trigger notification in Hunter is not the same as the event notification in applicant's disclosure. Furthermore, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate the trigger event to be sent to the camera. Furthermore, in Hunter, the camera acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where the data capture device acquires new-data immediately after the paired short-range wireless connection is established (without any phone call trigger event from the mobile device). **Furthermore, in Hunter, the trigger event or signal is sent from the mobile device to the camera, and image capture occurs after receiving the trigger event. This is in direct contrast to applicant's disclosure**, where, after acquiring the new-data, the data capture device sends the

LifeScan, Inc. Ex. 1006
Page 116 of 353
IPR2025-00102

notification signal to the mobile device informing the mobile device that it has acquired the new-data.

Argument #9:

Phone call Trigger event in Hunter (see paragraphs [0036], [0038], [0043]) over NON paired connection

As illustrated before, in Hunter, there is no cryptographic authentication of the mobile device by the camera. Furthermore, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate the trigger event or signal to be sent to the camera. Furthermore, in Hunter, the camera acquires the new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where the data capture device acquires the new-data immediately after a paired short-range wireless connection is established (without any phone call trigger event from the mobile device). Furthermore, in Hunter, the phone call trigger event or signal is sent from the mobile device to the camera. This is in direct contrast to applicant's disclosure, where, after acquiring the new-data, the data capture device sends the notification signal and the acquired new-data to the mobile device.

Argument #10:

Use HTTP to transfer new-data and a user authentication credential to website

In applicant's invention, the cellular phone uses HTTP to transfer new-data and a user authentication credential to website. Neither Hunter nor Pietruszka teach or suggest the use of HTTP to transfer the new-data and the user authentication credential to the website.

LifeScan, Inc. Ex. 1006
Page 117 of 353
IPR2025-00102

In view of above arguments 8-10, applicant submits that Hunter, in view of Pietruszka does not teach or suggest the following limitation in claim 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, 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, 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, wherein a 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, wherein the 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, 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 and the user authentication credential to a user data publishing website over a cellular data network, and wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data."

Argument #11:

None of the cited prior art show the Claim 12 Polling limitation of:

LifeScan, Inc. Ex. 1006
Page 118 of 353
IPR2025-00102

Short-range wireless enabled cellular phone sends a polling request to a short-range wireless enabled data capture device, over an established paired short-range wireless connection, to detect new-data for transfer from the short-range wireless enabled data capture device to the paired and cryptographically authenticated short-range wireless enabled cellular phone

As illustrated before, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate the trigger event or signal to be sent to the camera. Furthermore, in Hunter, the camera acquires the new-data only after it receives the trigger event or signal from the mobile device. In contrast, in applicant's disclosure, **the polling request from the mobile phone to the camera is for detecting already acquired new data.**

LifeScan, Inc. Ex. 1006
Page 119 of 353
IPR2025-00102

Summary

Comparison Table

	Claim Feature	Hunter	Pietruszka	Applicant Cellspin
1	Pairing for new-data transfer.	NO mention of pairing. Pairing is NOT established. Teaching away from establishing permanent connection.	NO Invention is about selecting or preventing, and controlling pairing between devices. NOT for new-data transfer	YES Pairing is established to transfer the acquired new-data.
2	Cryptographically authenticate the identity of Mobile Device	NO	YES Only if wireless communication device is unlocked for pairing.	YES The Mobile device is cryptographically authenticated by the data capture device NOT based on pre-selection of activation or deactivation of pairing.
3	Sending new data capture Event Notification Signal	NO Trigger Event Signal is sent from the mobile device to the camera device, which is opposite to applicant's invention.	NO There is NO data capture Event signal sent to the cellular phone. There is NO data capture device.	YES Event Notification signal is sent from data capture device to cellular phone after acquiring new data.
4	Send data to the mobile device over a pre-established paired connection	NO	NO There is no data to transfer.	YES
4	HTTP based transfer	NO HTTP is NOT used	NO There is No data to transfer.	YES HTTP is used as a data transport protocol
5	Is Timing of Data Acquisition after Pairing devices	NO	NO	YES After pairing is established
6	Data transfer between two devices happens over what type of wireless link?	NON-Paired wireless connection	NO data There is no new data to transfer	Data over Paired wireless connection

In view of the above arguments, Hunter, in view of Pietruszka does not teach or suggest all the limitations in claims 1, 4, 8 and 12.

Therefore, claims 1, 4, 8 and 12 are non-obvious over Hunter, in view of Pietruszka. Claims 2-3 are dependent on claim 1; claims 5-6 are dependent on claim 4; claim 9 is dependent on claim 8; claim 13 is dependent on claim 12. Applicant therefore respectfully submits that dependent claims 2-3, 5-6, 9 and 13 are also non-obvious over Hunter, in view of Pietruszka.

Applicant therefore respectfully requests that the rejection of claims 1-6, 8-9 and 12-13 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

The office action further states: "**Claim 7 & 14 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778 further in view of Risbood US 20070111748**".

In an earlier part of this response, arguments were presented to show that Hunter, in view of Pietruszka, does not teach or suggest the following limitations in claim 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, 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;"
>
> "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;"
>
> "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, 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, 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

LifeScan, Inc. Ex. 1006
Page 121 of 353
IPR2025-00102

paired wireless connection, wherein a 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, wherein the 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, 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 and the user authentication credential to a user data publishing website over a cellular data network, and wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data."

Also, in an earlier part of this response, arguments were presented to show that Hunter, in view of Pietruszka does not teach or suggest the following limitations in claim 12:

"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;"

"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;"

"said processor further configured to listen to a polling request from a 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, wherein the 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 mobile client application on the short-range wireless enabled cellular phone, over the established paired short-range wireless connection;"

"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 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 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 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 mobile client application on the short-range wireless enabled cellular phone is further 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, and wherein the mobile client application on the short-range wireless enabled cellular phone provides a touch based GUI for the received new-data."

LifeScan, Inc. Ex. 1006
Page 123 of 353
IPR2025-00102

Risbood does not remedy the deficiencies in a combination of Hunter and Pietruszka.

Applicant therefore respectfully submits that Hunter, in view of Pietruszka, further in view of Risbood, does not teach or suggest the following limitations in claim 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, 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;"
>
> "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;"
>
> "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, 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, 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, wherein a 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

LifeScan, Inc. Ex. 1006
Page 124 of 353
IPR2025-00102

memory device of the cryptographically authenticated short-range wireless enabled cellular phone, wherein the 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, 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 and the user authentication credential to a user data publishing website over a cellular data network, and wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data."

Furthermore, applicant respectfully submits that Hunter, in view of Pietruszka, further in view of Risbood, does not teach or suggest the following limitations in claim 12:

"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;"

"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;"

"said processor further configured to listen to a polling request from a mobile client application on the short-range wireless enabled cellular phone, over the

LifeScan, Inc. Ex. 1006
Page 125 of 353
IPR2025-00102

established paired short-range wireless connection, wherein the polling request is for the new-data, wherein the 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 mobile client application on the short-range wireless enabled cellular phone, over the established paired short-range wireless connection;"

"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 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 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 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 mobile client application on the short-range wireless enabled cellular phone is further 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, and wherein the mobile client application on the short-range wireless enabled cellular phone provides a touch based GUI for the received new-data."

Claims 1 and 12 are therefore non-obvious over Hunter, in view of Pietruszka and Risbood. Claims 7 and 14 are dependent on claims 1 and 12 respectively. Since claims 1

LifeScan, Inc. Ex. 1006
Page 126 of 353
IPR2025-00102

and 12 are non-obvious over Hunter, in view of Pietruszka and Risbood, dependent claims 7 and 14 are also non-obvious over Hunter, in view of Pietruszka and Risbood. Applicant therefore respectfully requests that the rejection of claims 7 and 14 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case. In the interest of compact prosecution, if the prosecution of the application can be advanced, applicant requests Examiner Nooristany to call the undersigned with the proposed amendment.

Respectfully submitted,

Date: July 21, 2021

/Ash Tankha/
Ashok Tankha
Attorney For Applicant
Reg. No. 33,802

Correspondence Address
Lipton Weinberger & Husick
36 Greenleigh Drive
Sewell, NJ 08080
Phone: 856-266-5145
Email: ash@ipprocurement.com

LifeScan, Inc. Ex. 1006
Page 127 of 353
IPR2025-00102

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/532,507	08/06/2019	Gurvinder Singh	CellSpin_04Con17_US	6207

64188 7590 06/08/2021

ASHOK TANKHA
36 GREENLEIGH DRIVE
SEWELL, NJ 08080

EXAMINER	
NOORISTANY, SULAIMAN	

ART UNIT	PAPER NUMBER
2415	

NOTIFICATION DATE	DELIVERY MODE
06/08/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ASH@IPPROCUREMENT.COM
docketing1@ipprocurement.com
docketing@ipprocurement.com

PTOL-90A (Rev. 04/07)

LifeScan, Inc. Ex. 1006
Page 128 of 353
IPR2025-00102

Office Action Summary	Application No. 16/532,507	Applicant(s) Singh et al.	
	Examiner SULAIMAN NOORISTANY	Art Unit 2415	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 5/5/21.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-9 and 12-14 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-9 and 12-14 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☑ Interview Summary (PTO-413) Paper No(s)/Mail Date 5/27/21.

4) ☐ Other: _____.

a Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 7, 14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. More specifically, the applicant fails to sufficiently point out or describe ***use HTTP to send user preference to the user data publishing website over the cellular data network, wherein the user preference comprise global positioning system information***.

The specification of this application under examination does not contain subject matter to implement limitations, as cited in the following claims.

It is not apparent how "***authentication credentials use HTTP to send user preference to the user data publishing website over the cellular data network, wherein the user preference comprise global positioning system information***" *as* recited in claim 7, is determined.

Examiner has reviewed the specification of this application under examination (and OCR whole document) and could not find support for the additional limitations as claimed.

LifeScan, Inc. Ex. 1006
Page 130 of 353
IPR2025-00102

Specification Objection

The disclosure is objected to because of the following informalities; Examiner has reviewed the specification of this application under examination and could not find support for the additional limitations as claimed "***use HTTP to send user preference to the user data publishing website over the cellular data network, wherein the user preference comprise global positioning system information***". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 7, 14 are rejected under 112, second paragraph as being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention

In claim 7, the terms "***use HTTP to send user preference to the user data publishing website over the cellular data network, wherein the user preference comprise global positioning system information***" are not clear what these are in reference to. Also, the description of the present application fails to provide a clear and complete description on the invention as well as the above terms. However, the claims will be given a broad reasonable interpretation for the purposes of examination as best understood.

Claims 14 is rejected for similar reasons as stated for claim 7.

LifeScan, Inc. Ex. 1006
Page 131 of 353
IPR2025-00102

Claim Rejections - 35 USC § 103

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1-6, 8-9, 12-13 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778.

4. A system, comprising:

a short-range wireless enabled data capture device **(Hunter fig. 1, unit 10)**, comprising:

a first memory device **(Hunter: a camera with an image memory and a first wireless communication interface [0010] fig. 1, unit 10)**;

a first processor coupled to the first memory device **(Hunter: a camera with an image memory and a first wireless communication interface [0010] fig. 1, unit 10)**;

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 **(Hunter: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10**

LifeScan, Inc. Ex. 1006
Page 132 of 353
IPR2025-00102

to establish a data link between the two units. Alternatively, the camera 10 may periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10 [0017-0027, 0036-0037]).

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;

a data capture circuitry **(Hunter: fig. 1 unit 10)**;

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 **(Hunter: [0017-0027, 0036-0037] After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038])**;

said first processor further configured to store the new-data in the first memory device **(Hunter: After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038])**;

said first processor further configured to send an event notification **(Hunter: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event,**

LifeScan, Inc. Ex. 1006
Page 133 of 353
IPR2025-00102

and communicating with the other of the camera and the communications device by a wireless link therebetween [0013]) and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically **(Hunter: transferring images between the camera and the communications device over the wireless link [0013])**, 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 **(Hunter: [0013])**,

said short-range wireless enabled cellular phone **(Hunter: fig. 1 unit 20)**, comprising:

a second memory device **(Hunter: fig. 1 unit 20)**;

a second processor coupled to the second memory device **(Hunter: fig. 1 unit 20)**;

a cellular network communication device configured to connect to the internet via the cellular data network **(Hunter: fig. 1 unit 20)**;

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 **(Hunter: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10 to establish a data link between the two units. Alternatively, the camera 10 may periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10 [0017-0027, 0036-0037])**;

a 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 an event notification sent by the short-range wireless enabled data capture

LifeScan, Inc. Ex. 1006
Page 134 of 353
IPR2025-00102

device, wherein a mobile client application for the short-range wireless enabled cellular phone is configured to process the event notification **(Hunter: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween [0013])**;

receive the new-data from the short-range wireless enabled data capture device **(Hunter: an image storage buffer 24 for storing image data received from the camera 10 [0035])**;

store the received new-data in the second memory device **(Hunter: an image storage buffer 24 for storing image data received from the camera 10 [0035])**;

store the user authentication credential in the second memory device **(Hunter: The wireless link may be pre-existing, or may be set up only on the initiation of the call [0017-0027, 0036-0037, 0039-0040])**;

use HTTP to upload the received new-data and a user authentication credential to a user data publishing website over the cellular data network **(Hunter: transferring said images from the communications device on to a data network through a data network interface [0013, 0035, 0041])**;

provide a touch based graphical user interface for the received new-data **(Hunter: [0025])**

Hunter merely discloses the term *cryptographically* authenticating

Pietruszka further teaches cryptographically authenticating **(Pietruszka: [0037])**; store the user authentication credential in the second memory device **(Pietruszka fig. 9A-9D)** and provide a touch based graphical user interface for the received new-data **(Pietruszka [0099-**

LifeScan, Inc. Ex. 1006
Page 135 of 353
IPR2025-00102

0110]) in order to communicate only with a trusted device can cryptographically authenticate the identity of the other device.

Thus, it would have been obvious to one skill in the art to include the above recited limitation into Hunter's in order to communicate only with a trusted device can cryptographically authenticate the identity of the other device [0037], as taught by Pietruszka.

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 (**Hunter: [0037]**)

6. The system of claim 4, wherein the user authentication credential is for a user of the user data publishing website (**Hunter: [0025]**)

Claim 7 & 14 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778 further in view of Risbood US 20070111748

7. The system of claim 4, wherein data the mobile client application for the short-range wireless enabled cellular phone comprises executable instructions that, when executed by the second processor controls the second processor to: use HTTP to send user preference to the user data publishing website over the cellular data network, [[*wherein the user preference comprise global positioning system information*]] (**Hunter: [0031]**

LifeScan, Inc. Ex. 1006
Page 136 of 353
IPR2025-00102

Risbood further teaches wherein the user preference comprise global positioning system information **(Risbood: fig. 3, unit 340-350 [0027])** in order to connect directly to the resident server using the well-known HTTP or TCP/IP protocols, and with conventional authentication and encryption can upload the data

Thus, it would have been obvious to one skill in the art to include the above recited limitation into Hunter's invention in order to connect directly to the resident server using the well-known HTTP or TCP/IP protocols, and with conventional authentication and encryption can upload the data [0027], as taught by Risboot.

Regarding claims 1-3, 8-9, 12-14 the independent claim and each dependent claim are related to the same limitation set for hereinabove in claims 4-7, where the difference used is a "capture device" & "mobile device" and the wordings of the claims were interchanged within the claim itself or some of the claims were presented as a combination of two or more previously presented limitations. This change does not affect the limitation of the above treated claims. Adding these phrases to the claims and interchanging the wording did not introduce new limitations to these claims. Therefore these claims were rejected for similar reasons as stated above

Response to Arguments

Applicant's arguments filed on 05/05/21 have been fully considered but they are not persuasive.

Applicant Argument:

LifeScan, Inc. Ex. 1006
Page 137 of 353
IPR2025-00102

Regarding first paragraph of 35 U.S.C. 112 rejection, Applicant is suggesting for support to some page Nos. 5, 7, 9 and Figure 2 and Figure 4 of US Non-provisional patent application serial number 11/901,802.

Response to Arguments:

With respect to the above argument, Examiner would like to draw attention that the US Non-provisional patent application serial number 11/901,802 or any other cross reference related Applications does not support the limitation of claim 7 & 14. Thus, the Examiner maintains the rejection.

Applicant Argument: 1

Prior art failed to teach *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, 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.*

Response to Arguments:

In addition, the Examiner would like to draw attention to (fig. 1, [0013]) of **Hunter**, for example: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link

LifeScan, Inc. Ex. 1006
Page 138 of 353
IPR2025-00102

therebetween... The Examiner further would like to draw attention to ([0017-0027, 0036-0037-0038]) of **Hunter**, for example - After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038] (*herein* **it's** considered same as *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, 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*).

Applicant Argument: 2

Prior art failed to teach "*wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data*"

Response to Arguments:

In addition, the Examiner would like to draw attention to (fig. 8, 9A-9D, [0099-0110]) of **Pietruszka**, for example: As shown in FIG. 8, user interface 814 is also coupled to processor 810. User interface 814 facilitates the exchange of information with a user. FIG. 8 shows that user interface 814 includes a user input portion 820 and a user output portion 822. User input portion 820 may include one or more components that allow a user to input information. Examples of such components include keypads, touch screens, and microphones. User output

LifeScan, Inc. Ex. 1006
Page 139 of 353
IPR2025-00102

portion 822 allows a user to receive information from the device. Thus, user output portion 822 may include various components, such as a display, and one or more audio speakers. Exemplary displays include liquid crystal displays (LCDs), and video displays. The user interface 814 can allow a user to perform various tasks including among other things those tasks associated with the security or protection embodiments described herein, including for example setting or changing of the operational state (e.g., Locked, Unlocked, Selective, etc.) of the device or other remote devices, entering or changing passwords, and so forth……(*herein* **it's** considered same as *wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data*).

Applicant Argument: 3-5

Prior art failed to teach *pairing short range wireless or away from permanent paired short-range wireless connection and cryptographic pairing between devices*

Response to Arguments:

With respect to the above argument, Examiner would like to draw attention to that **it is the claims that define the claimed invention, and it is claims, not specifications that are anticipated or unpatentable. Constant v. Advanced Micro-Devices Inc., 7 USPQ2d 1064**.

In addition, the Examiner would like to draw attention to (fig. 1, [0017-0027, 0036-0037]) of **Hunter**, for example: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10 to establish a data link between the two units. Alternatively, the camera 10 may periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10.

LifeScan, Inc. Ex. 1006
Page 140 of 353
IPR2025-00102

The Examiner further would like to draw attention to ([0037]) of **Hunter**, for example: a device that wishes to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt data exchanged over a wireless medium as an added security. The encryption can however be turned off and passkeys can be stored on the device's file system rather than the Bluetooth component or chip itself. Since the Bluetooth address can be permanent, a pairing can be preserved even if the Bluetooth name is changed. Either device in a pairing relationship may delete the pairing between the devices. Devices may require pairing or may prompt the user before it allows a remote device to utilize any or all or some of its services (*herein* **it's** considered same as *paired short-range wireless connection and cryptographic pairing between devices*).

Furthermore, the Examiner would like to draw attention to (fig. 1-9) of **Pietruszka**, for example: Accordingly, FIG. 1 is a diagram of an exemplary operational environment 100. This environment includes one or more wireless communications devices (WCDs), such as WCD 110 and WCD 120, which can establish trusted relationships with each other or with other devices to facilitate subsequent wireless communications between the trusted devices and/or set or change an operational state of device pertaining to the handling of the establishment of trusted relationships with other devices. As shown, WCD 110 includes operational state(s) which control its ability to establish a trusted relationship with other devices, such as WCD 120 or other devices. As shown by reference to numeral 112, the operational states may include a locked state to prevent (or prohibit) establishing of a trusted relationship with a remote device or an unlocked state to allow establishing of a trusted relationship with a remote device. Other operational states may also be included such as a selective state, e.g., selective locked or selective unlocked, in which a particular subset or type of device, which may be defined by some discernable category

LifeScan, Inc. Ex. 1006
Page 141 of 353
IPR2025-00102

or characteristic (e.g., manufacturer, type of device, and so forth), may be allowed or prevented from establishing a trusted relationship. The operational states may be implemented through a security application resident in one or both of WCD 110, 120 (*herein* **it's** considered same as *paired short-range wireless connection and cryptographic pairing between devices*).

Applicant Argument: 6

Prior art failed to teach *receiving or making Phone call trigger even vs NO such Phone call trigger event.*

Response to Arguments:

In addition, the Examiner would like to draw attention to (fig. 1, [0013]) of **Hunter**, for example: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween (*herein* **it's** considered same as *sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data*).

Applicant Argument: 7

Prior art failed to teach setting based control of cryptographic pairing between devices in NOT relevant in application's scenario

Response to Arguments:

LifeScan, Inc. Ex. 1006
Page 142 of 353
IPR2025-00102

The Examiner further would like to draw attention to ([0017-0027, 0036-0037-0038]) of **Hunter**, for example - After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038].

In addition, the Examiner would like to draw attention to (fig. 1-9, [0024-0025]) of **Pietruszka**, for example: Accordingly, FIG. 1 is a diagram of an exemplary operational environment 100. This environment includes one or more wireless communications devices (WCDs), such as WCD 110 and WCD 120, which can establish trusted relationships with each other or with other devices to facilitate subsequent wireless communications between the trusted devices and/or set or change an operational state of device pertaining to the handling of the establishment of trusted relationships with other devices. As shown, WCD 110 includes operational state(s) which control its ability to establish a trusted relationship with other devices, such as WCD 120 or other devices. As shown by reference to numeral 112, the operational states may include a locked state to prevent (or prohibit) establishing of a trusted relationship with a remote device or an unlocked state to allow establishing of a trusted relationship with a remote device. Other operational states may also be included such as a selective state, e.g., selective locked or selective unlocked, in which a particular subset or type of device, which may be defined by some discernable category or characteristic (e.g., manufacturer, type of device, and so forth), may be allowed or prevented from establishing a trusted relationship. The operational states may be implemented through a security application resident in one or both of WCD 110, 120 (*herein* **it's** considered same as *cryptographically authenticated short-range wireless that is based control of cryptographic pairing between devices in relevant in application's scenario*).

Applicant Argument: 8-9

Prior art failed to teach Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data.

Response to Arguments:

In addition, the Examiner would like to draw attention to (fig. 1, [0013]) of **Hunter**, for example: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween (*herein* **it's** considered same as *Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data*).

In addition, the Examiner would like to draw attention to (fig. 1, [0017-0027, 0036-0037]) of **Hunter**, for example: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10 to establish a data link between the two units. Alternatively, the camera 10 may periodically transmit a signal which is received and

LifeScan, Inc. Ex. 1006
Page 144 of 353
IPR2025-00102

acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10.

The Examiner further would like to draw attention to ([0037]) of **Hunter**, for example: a device that wishes to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt data exchanged over a wireless medium as an added security. The encryption can however be turned off and passkeys can be stored on the device's file system rather than the Bluetooth component or chip itself. Since the Bluetooth address can be permanent, a pairing can be preserved even if the Bluetooth name is changed. Either device in a pairing relationship may delete the pairing between the devices. Devices may require pairing or may prompt the user before it allows a remote device to utilize any or all or some of its services…

The Examiner further would like to draw attention to ([0017-0027, 0036-0037-0038]) of **Hunter**, for example - After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone (*herein* **it's** considered same as *Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data*).

Applicant Argument: 10

LifeScan, Inc. Ex. 1006
Page 145 of 353
IPR2025-00102

Prior art failed to teach use HTTP to transfer new-data and a user authentication credential to website

Response to Arguments:

In addition, the Examiner would like to draw attention to (fig. 1, [0009, 0031, 0041]) of **Hunter**, for example: it is known for mobile telephones to support data instead of or as well as voice calls, in which case the present invention can be taken to relate also to the establishment of a data link or the initiation of data transmission as a result of use of a telephone to access a data service, e.g. an internet page such as a photo website or a photo printing service (*herein* **it's** considered same as *use HTTP to transfer new-data and a user authentication credential to website*).

Applicant Argument: 11

Prior art failed to teach the Claim 12 Polling limitation of: Short-range wireless enabled cellular phone sends a polling request to a short-range wireless enabled data capture device, over an established paired short-range wireless connection, to detect new-data for transfer from the short-range wireless enabled data capture device to the paired and cryptographically authenticated short-range wireless enabled cellular phone

Response to Arguments:

The Examiner would like to draw attention to (fig. 1, [0013]) of **Hunter**, for example: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and

LifeScan, Inc. Ex. 1006
Page 146 of 353
IPR2025-00102

communicating with the other of the camera and the communications device by a wireless link therebetween..

The Examiner further would like to draw attention to ([0017-0027, 0036-0037-0038]) of **Hunter**, for example - After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038] (*herein* **it's** considered same as *the Claim 12 Polling limitation of…*)

Thus, for the above reason, the prior art meet the claim limitation.

The examiner stresses that the claims are too broad and require detail or specialization of the steps as recited in the claims. Alone and as claimed, the limitations are too open.

Examiner has cited particular portions of the references as applied to each claim limitation for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

LifeScan, Inc. Ex. 1006
Page 147 of 353
IPR2025-00102

Regarding all other arguments presented by applicant, the arguments are substantially the same as those which have already been addressed above and in the interest of brevity; the Examiner directs the applicant to those responses above.

Remark:

In addition, an interview could expedite the prosecution.

Conclusion

Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sulaiman Nooristany whose telephone number is 571-270-1929. The examiner can normally be reached on Monday thru Friday: 8:30am to 5:00pm (EST). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Rutkowski can be reached on 571-270-1215. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an

LifeScan, Inc. Ex. 1006
Page 148 of 353
IPR2025-00102

application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/SULAIMAN NOORISTANY/

Primary Examiner, Art Unit 2415

LifeScan, Inc. Ex. 1006
Page 149 of 353
IPR2025-00102

Amendments to the claims

Claim 1 (previously presented): A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device;

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, wherein the event notification corresponds to the acquired new-data and comprises sending a signal to the cryptographically authenticated short-

LifeScan, Inc. Ex. 1006
Page 150 of 353
IPR2025-00102

range wireless enabled cellular phone, 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, wherein a 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, wherein the 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, 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 and the user authentication credential to a user data publishing website over a cellular data network, and wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data.

Claim 2 (previously presented): 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.

Claim 3 (previously presented): The short-range wireless enabled data capture device of claim 1, wherein the user authentication credential sent by the 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.

Claim 4 (previously presented): A system, comprising:

a short-range wireless enabled data capture device, comprising:

LifeScan, Inc. Ex. 1006
Page 151 of 353
IPR2025-00102

a first memory device;

a first processor coupled to the first memory device;

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;

a data capture circuitry;

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;

said first processor further configured to store the new-data in the first memory device; and

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;

LifeScan, Inc. Ex. 1006
Page 152 of 353
IPR2025-00102

said short-range wireless enabled cellular phone, comprising:

a second memory device;

a second processor coupled to the second memory device;

a cellular network communication device configured to connect to the internet via a cellular data network;

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;

a 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, wherein the mobile client application for the short-range wireless enabled cellular phone is configured to process the event notification;

receive the new-data from the short-range wireless enabled data capture device;

store the received new-data in the second memory device;

store a user authentication credential in the second memory device;

5

LifeScan, Inc. Ex. 1006
Page 153 of 353
IPR2025-00102

use HTTP to upload the received new-data and the user authentication credential to a user data publishing website over the cellular data network; and

provide a touch based graphical user interface for the received new-data.

Claim 5 (previously presented): 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.

Claim 6 (previously presented): The system of claim 4, wherein the user authentication credential is for a user of the user data publishing website.

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

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

Claim 8 (previously presented): A short-range wireless enabled cellular phone, comprising:

a memory device;

a processor coupled to the memory device;

LifeScan, Inc. Ex. 1006
Page 154 of 353
IPR2025-00102

a cellular network communication device configured to connect to internet via a cellular data network;

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;

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:

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;

receive the event notification and the new-data from the short-range wireless enabled data capture device;

process the event notification and store the received new-data in the memory device;

store a user authentication credential in the memory device;

LifeScan, Inc. Ex. 1006
Page 155 of 353
IPR2025-00102

use HTTP to upload the received new-data and the user authentication credential to a user data publishing web service over the cellular data network; and

provide a touch based graphical user interface for the received new-data.

Claim 9 (previously presented): The short-range wireless enabled cellular phone of claim 8, 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.

Claims 10-11 (cancelled).

Claim 12 (previously presented): A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device of the short-range wireless enabled data capture device;

said processor further configured to listen to a polling request from a 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, wherein the 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 mobile client application on the short-range wireless enabled cellular phone, over the established paired short-range wireless connection;

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 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 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 mobile client application for the short-range wireless enabled cellular phone stores a user authentication credential in the memory device of the

LifeScan, Inc. Ex. 1006
Page 157 of 353
IPR2025-00102

short-range wireless enabled cellular phone, wherein the mobile client application on the short-range wireless enabled cellular phone is further 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, and wherein the mobile client application on the short-range wireless enabled cellular phone provides a touch based GUI for the received new-data.

Claim 13 (previously presented): The short-range wireless enabled data capture device of claim 12, 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.

Claim 14 (currently amended): The short-range wireless enabled data capture device of claim 12, wherein the mobile client application for the short-range wireless enabled cellular phone uses HTTP to send user preferences ~~global positioning system information~~ to the user data publishing web service over the cellular data network, wherein the user preferences comprise global positioning system information.

LifeScan, Inc. Ex. 1006
Page 158 of 353
IPR2025-00102

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed	PTO/SB/25 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION**
Application Number	16532507
Filing Date	06-Aug-2019
First Named Inventor	Gurvinder Singh
Attorney Docket Number	CellSpin_04Con17_US
Title of Invention	Automatic Multimedia Upload For Publishing Data And Multimedia Content

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
CellSpinSoft Inc.	100%

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

15659637 filed on 07/26/2017
11901802 filed on 09/19/2007
14503401 filed on 10/01/2014
14273546 filed on 05/09/2014
14172913 filed on 02/05/2014
14576202 filed on 12/19/2014
13740214 filed on 01/13/2013
12333303 filed on 12/11/2008

LifeScan, Inc. Ex. 1006
Page 159 of 353
IPR2025-00102

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

- (●) Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.
- ( ) I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicant claims the following fee status:

- (●) Small Entity
- ( ) Micro Entity
- ( ) Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further 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 Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

- (●) An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

  Registration Number 33802
- ( ) A sole inventor
- ( ) A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application
- ( ) A joint inventor; all of whom are signing this request

Signature	/a tankha/
Name	Ashok Tankha

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

LifeScan, Inc. Ex. 1006
Page 160 of 353
IPR2025-00102

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 16532507

Filing Date: 06-Aug-2019

Applicant/Patent under Reexamination: Singh

Electronic Terminal Disclaimer filed on May 5, 2021

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

LifeScan, Inc. Ex. 1006
Page 161 of 353
IPR2025-00102

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/532,507	08/06/2019	Gurvinder Singh	CellSpin_04Con17_US	6207

64188 7590 02/09/2021
ASHOK TANKHA
36 GREENLEIGH DRIVE
SEWELL, NJ 08080

EXAMINER
NOORISTANY, SULAIMAN

ART UNIT	PAPER NUMBER
2415	

NOTIFICATION DATE	DELIVERY MODE
02/09/2021	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ASH@IPPROCUREMENT.COM
docketing1@ipprocurement.com
docketing@ipprocurement.com

PTOL-90A (Rev. 04/07)

LifeScan, Inc. Ex. 1006
Page 162 of 353
IPR2025-00102

Office Action Summary	Application No. 16/532,507	Applicant(s) Singh et al.	
	Examiner SULAIMAN NOORISTANY	Art Unit 2415	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 1/20/21.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-9 and 12-14 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-9 and 12-14 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

aNotice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 7 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

LifeScan, Inc. Ex. 1006
Page 164 of 353
IPR2025-00102

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claims 1-9, 12-14 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claims of parent Application(s) No. **15659637, 14578202, 14503401, 14273546, 14172913, 13740214, 12333303** and co-pending Application No. **11901802**. Although the claims at issue are identical, they are not patentably distinct from each other because they are same variants of each other.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

LifeScan, Inc. Ex. 1006
Page 165 of 353
IPR2025-00102

Claims 7, 14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. More specifically, the applicant fails to sufficiently point out or describe ***use HTTP to send global positioning system information to the user data publishing website over the cellular data network***.

The specification of this application under examination does not contain subject matter to implement limitations, as cited in the following claims.

It is not apparent how "***authentication credentials use HTTP to send global positioning system information to the user data publishing website over the cellular data network***" *as* recited in claim 7, is determined.

Examiner has reviewed the specification of this application under examination (and OCR whole document) and could not find support for the additional limitations as claimed.

Specification Objection

The disclosure is objected to because of the following informalities: Examiner has reviewed the specification of this application under examination and could not find support for the additional limitations as claimed "***use HTTP to send global positioning system information to the user data publishing website over the cellular data network***". Appropriate correction is required.

LifeScan, Inc. Ex. 1006
Page 166 of 353
IPR2025-00102

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 7, 14 are rejected under 112, second paragraph as being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention

In claim 7, the terms "***use HTTP to send global positioning system information to the user data publishing website over the cellular data network***" are not clear what these are in reference to. Also, the description of the present application fails to provide a clear and complete description on the invention as well as the above terms. However, the claims will be given a broad reasonable interpretation for the purposes of examination as best understood.

Claims 14 is rejected for similar reasons as stated for claim 7.

Claim Rejections - 35 USC § 103

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

LifeScan, Inc. Ex. 1006
Page 167 of 353
IPR2025-00102

Claim 1-9, 12-14 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778.

4. A system, comprising:

a short-range wireless enabled data capture device **(Hunter fig. 1, unit 10)**, comprising:

a first memory device **(Hunter: a camera with an image memory and a first wireless communication interface [0010] fig. 1, unit 10)**;

a first processor coupled to the first memory device **(Hunter: a camera with an image memory and a first wireless communication interface [0010] fig. 1, unit 10)**;

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 **(Hunter: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10 to establish a data link between the two units. Alternatively, the camera 10 may periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10 [0017-0027, 0036-0037])**,

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;

a data capture circuitry **(Hunter: fig. 1 unit 10)**;

LifeScan, Inc. Ex. 1006
Page 168 of 353
IPR2025-00102

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 **(Hunter: [0017-0027, 0036-0037] After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038])**;

said first processor further configured to store the new-data in the first memory device **(Hunter: After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038])**;

said first processor further configured to send an event notification **(Hunter: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween [0013])** and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically **(Hunter: transferring images between the camera and the communications device over the wireless link [0013])**, 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 **(Hunter: [0013])**.

said short-range wireless enabled cellular phone **(Hunter: fig. 1 unit 20)**, comprising:

LifeScan, Inc. Ex. 1006
Page 169 of 353
IPR2025-00102

a second memory device **(Hunter: fig. 1 unit 20)**;

a second processor coupled to the second memory device **(Hunter: fig. 1 unit 20)**;

a cellular network communication device configured to connect to the internet via the cellular data network **(Hunter: fig. 1 unit 20)**;

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 **(Hunter: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10 to establish a data link between the two units. Alternatively, the camera 10 may periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10 [0017-0027, 0036-0037])**;

a 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 an event notification sent by the short-range wireless enabled data capture device, wherein a mobile client application for the short-range wireless enabled cellular phone is configured to process the event notification **(Hunter: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween [0013])**;

receive the new-data from the short-range wireless enabled data capture device **(Hunter: an image storage buffer 24 for storing image data received from the camera 10 [0035])**;

LifeScan, Inc. Ex. 1006
Page 170 of 353
IPR2025-00102

store the received new-data in the second memory device **(Hunter: an image storage buffer 24 for storing image data received from the camera 10 [0035])**;

store the user authentication credential in the second memory device **(Hunter: The wireless link may be pre-existing, or may be set up only on the initiation of the call [0017-0027, 0036-0037, 0039-0040])**;

use HTTP to upload the received new-data and a user authentication credential to a user data publishing website over the cellular data network **(Hunter: transferring said images from the communications device on to a data network through a data network interface [0013, 0035, 0041])**;

provide a touch based graphical user interface for the received new-data **(Hunter: [0025], Pietruszka [0099])**

Hunter merely discloses the term *cryptographically* authenticating

Pietruszka further teaches cryptographically authenticating **(Pietruszka: [0037])**; store the user authentication credential in the second memory device **(Pietruszka fig. 9A-9D)** and provide a touch based graphical user interface for the received new-data **(Pietruszka [0099])** in order to communicate only with a trusted device can cryptographically authenticate the identity of the other device.

Thus, it would have been obvious to one skill in the art to include the above recited limitation into Hunter's in order to communicate only with a trusted device can cryptographically authenticate the identity of the other device [0037], as taught by Pietruszka.

LifeScan, Inc. Ex. 1006
Page 171 of 353
IPR2025-00102

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 **(Hunter: [0037])**

6. The system of claim 4, wherein wherein the user authentication credential is for a user of the user data publishing website **(Hunter: [0025])**

7. The system of claim 4, wherein data the mobile client application for the short-range wireless enabled cellular phone comprises executable instructions that, when executed by the second processor controls the second processor to: use HTTP to send global positioning system information to the user data publishing website over the cellular data network **(Hunter: [0031])**

Regarding claims 1-3, 8-9, 12-14 the independent claim and each dependent claim are related to the same limitation set for hereinabove in claims 4-7, where the difference used is a "capture device" & "mobile device" and the wordings of the claims were interchanged within the claim itself or some of the claims were presented as a combination of two or more previously presented limitations. This change does not affect the limitation of the above treated claims. Adding these phrases to the claims and interchanging the wording did not introduce new limitations to these claims. Therefore these claims were rejected for similar reasons as stated above

Response to Arguments

Applicant's arguments filed on 01/20/21 have been fully considered but they are not persuasive.

LifeScan, Inc. Ex. 1006
Page 172 of 353
IPR2025-00102

Applicant Argument:

Regarding first paragraph of 35 U.S.C. 112 rejection, Applicant is suggesting for support to some page Nos. 5, 7, 9 and Figure 2 and Figure 4 of US Non-provisional patent application serial number 11/901,802.

Response to Arguments:

With respect to the above argument, Examiner would like to draw attention that the US Non-provisional patent application serial number 11/901,802 does not support the limitation of claim 7 & 14. Thus, the Examiner maintains the rejection.

Applicant Argument:

Prior art failed to teach pairing short range wireless or away from permanent paired short-range wireless connection and cryptographic pairing between devices…Also, the Prior arts setting based control of cryptographic pairing between devices is/are not relevant in applicant's scenario

Response to Arguments:

With respect to the above argument, Examiner would like to draw attention to that **it is the claims that define the claimed invention, and it is claims, not specifications that are anticipated or unpatentable. Constant v. Advanced Micro-Devices Inc., 7 USPQ2d 1064**.

In addition, the Examiner would like to draw attention to (fig. 1, [0017-0027, 0036-0037]) of **Hunter**, for example: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10 to establish a data link between the

LifeScan, Inc. Ex. 1006
Page 173 of 353
IPR2025-00102

two units. Alternatively, the camera 10 may periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10.

The Examiner further would like to draw attention to ([0037]) of **Hunter**, for example: a device that wishes to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt data exchanged over a wireless medium as an added security. The encryption can however be turned off and passkeys can be stored on the device's file system rather than the Bluetooth component or chip itself. Since the Bluetooth address can be permanent, a pairing can be preserved even if the Bluetooth name is changed. Either device in a pairing relationship may delete the pairing between the devices. Devices may require pairing or may prompt the user before it allows a remote device to utilize any or all or some of its services (*herein* **it's** considered same as *paired short-range wireless connection and cryptographic pairing between devices*).

Applicant Argument:

Prior art failed to teach sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data.

Response to Arguments:

LifeScan, Inc. Ex. 1006
Page 174 of 353
IPR2025-00102

In addition, the Examiner would like to draw attention to (fig. 1, [0013]) of **Hunter**, for example: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween (*herein* **it's** considered same as *sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data*).

Applicant Argument:

Prior art failed to teach receiving or making Phone call trigger even vs NO such Phone call trigger event.

Response to Arguments:

In addition, the Examiner would like to draw attention to (fig. 1, [0013]) of **Hunter**, for example: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween (*herein* **it's** considered same as *sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data*).

Applicant Argument:

LifeScan, Inc. Ex. 1006
Page 175 of 353
IPR2025-00102

Prior art failed to teach use HTTP to transfer new-data and a user authentication credential to website

Response to Arguments:

In addition, the Examiner would like to draw attention to (fig. 1, [0009, 0031, 0041]) of **Hunter**, for example: it is known for mobile telephones to support data instead of or as well as voice calls, in which case the present invention can be taken to relate also to the establishment of a data link or the initiation of data transmission as a result of use of a telephone to access a data service, e.g. an internet page such as a photo website or a photo printing service (*herein* **it's** considered same as *use HTTP to transfer new-data and a user authentication credential to website*).

Thus, for the above reason, the prior art meet the claim limitation.

The examiner stresses that the claims are too broad and require detail or specialization of the steps as recited in the claims. Alone and as claimed, the limitations are too open.

Examiner has cited particular portions of the references as applied to each claim limitation for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part

LifeScan, Inc. Ex. 1006
Page 176 of 353
IPR2025-00102

of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Regarding all other arguments presented by applicant, the arguments are substantially the same as those which have already been addressed above and in the interest of brevity; the Examiner directs the applicant to those responses above.

Remark:

In addition, an interview could expedite the prosecution.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sulaiman Nooristany whose telephone number is 571-270-1929. The examiner can normally be reached on Monday thru Friday: 8:30am to 5:00pm (EST). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Rutkowski can be reached on 571-270-1215. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from

LifeScan, Inc. Ex. 1006
Page 177 of 353
IPR2025-00102

a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/SULAIMAN NOORISTANY/

Primary Examiner, Art Unit 2415

LifeScan, Inc. Ex. 1006
Page 178 of 353
IPR2025-00102

Doc code. RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	16/532,507	Filing Date	2019-08-06	Docket Number (if applicable)	CellSpin_04Con17_US	Art Unit	2415
First Named Inventor	Gurvinder Singh			Examiner Name	Nooristany, Sulaiman		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 600314

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

X Patent Practitioner Signature

Applicant Signature

EFS - Web 2.1.16

LifeScan, Inc. Ex. 1006
Page 179 of 353
IPR2025-00102

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/a tankha/	Date (YYYY-MM-DD)	2021-01-20
Name	Ashok Tankha	Registration Number	33802

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re. application of:
Gurvinder Singh
Application No.: 16/532,507 Examiner: Nooristany, Sulaiman
Filed: 08/06/2019 Art Unit: 2415
Applicant: Cellspinsoft Inc. Atty. Docket no.: CellSpin_04Con17_US
Title: Automatic Multimedia Upload
For Publishing Data And Multimedia Content

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Request for continued examination

Examiner Nooristany:

In response to the final office action mailed October 26, 2020, please amend the above-referenced application as follows:

Amendments to the Claims are listed on page 2 of this response.

Remarks begin on page 12 of this response.

LifeScan, Inc. Ex. 1006
Page 182 of 353
IPR2025-00102

Amendments to the claims

Claim 1 (currently amended): A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device~~, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the created new-data~~;

said processor further configured to send an event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled

LifeScan, Inc. Ex. 1006
Page 183 of 353
IPR2025-00102

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, 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, wherein a 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, wherein the 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, 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 and [[a]] the user authentication credential to a user data publishing website over a cellular data network, and wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data.

Claim 2 (previously presented): 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.

Claim 3 (currently amended): The short-range wireless enabled data capture device of claim 1~~, wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone stores the user authentication credential in a non-volatile memory device of the cryptographically authenticated short-range wireless enabled cellular phone~~, wherein the user authentication credential sent by the mobile

LifeScan, Inc. Ex. 1006
Page 184 of 353
IPR2025-00102

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~~, and wherein the mobile client application provides a touch based GUI for the received new-data~~.

Claim 4 (currently amended): A system, comprising:

a short-range wireless enabled data capture device, comprising:

a first memory device;

a first processor coupled to the first memory device;

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;

a data capture circuitry;

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;

said first processor further configured to store the new-data in the first memory device~~, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device~~

LifeScan, Inc. Ex. 1006
Page 185 of 353
IPR2025-00102

~~and the short-range wireless enabled cellular phone remains paired after storing the created new-data~~; and

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;

said short-range wireless enabled cellular phone, comprising:

a second memory device;

a second processor coupled to the second memory device;

a cellular network communication device configured to connect to the internet via a cellular data network;

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;

a 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, wherein the mobile client application for the ~~cryptographically authenticated~~ short-range wireless

LifeScan, Inc. Ex. 1006
Page 186 of 353
IPR2025-00102

enabled cellular phone is configured to process the event notification;

receive the new-data from the short-range wireless enabled data capture device;

store the received new-data in the second memory device~~, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the received new-data~~; [[and]]

store a user authentication credential in the second memory device;

use HTTP to upload the received new-data and [[a]] the user authentication credential to a user data publishing website over the cellular data network; and

provide a touch based graphical user interface for the received new-data.

Claim 5 (previously presented): 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.

Claim 6 (currently amended): The system of claim 4, wherein the ~~mobile client application for the short-range wireless enabled cellular phone comprises executable instructions that, when executed by the second processor controls the second processor to:~~

LifeScan, Inc. Ex. 1006
Page 187 of 353
IPR2025-00102

~~store the user authentication credential in the second memory device, wherein the~~ user authentication credential is for a user of the user data publishing website~~; and~~

~~provide a touch based graphical user interface for the received new data~~.

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

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

Claim 8 (currently amended): A short-range wireless enabled cellular phone, comprising:

a memory device;

a processor coupled to the memory device;

a cellular network communication device configured to connect to internet via a cellular data network;

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~~;

LifeScan, Inc. Ex. 1006
Page 188 of 353
IPR2025-00102

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:

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 ~~cryptographically authenticated~~ 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;

receive the event notification and the new-data from the short-range wireless enabled data capture device;

process the event notification and store the received new-data in the memory device~~, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the received new-data~~; [[and]]

store a user authentication credential in the memory device;

use HTTP to upload the received new-data and [[a]] the user authentication credential to a user data publishing web service over the cellular data network; and

provide a touch based graphical user interface for the received new-data.

Claim 9 (previously presented): The short-range wireless enabled cellular phone of claim 8, wherein the short-range paired wireless connection is one of a Bluetooth paired

LifeScan, Inc. Ex. 1006
Page 189 of 353
IPR2025-00102

wireless connection, a Wi-Fi paired wireless connection, and other wireless personal area networking technologies that use pairing.

Claims 10-11 (cancelled).

Claim 12 (currently amended): A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device of the short-range wireless enabled data capture device~~, wherein the established short-range paired wireless connection between the short-range wireless enabled~~

LifeScan, Inc. Ex. 1006
Page 190 of 353
IPR2025-00102

~~data capture device and the short-range wireless enabled cellular phone remains paired after storing the created new-data~~;

said processor further configured to listen to a polling request from a mobile client application on the ~~cryptographically authenticated~~ short-range wireless enabled cellular phone, over the established paired short-range wireless connection, wherein the polling request is for the new-data, wherein the mobile client application on the ~~cryptographically authenticated~~ 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 mobile client application on the ~~cryptographically authenticated~~ short-range wireless enabled cellular phone, over the established paired short-range wireless connection;

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 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 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 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 mobile client application on the short-range wireless enabled cellular phone is further configured to use

LifeScan, Inc. Ex. 1006
Page 191 of 353
IPR2025-00102

HTTP to upload the received new-data and [[a]] the user authentication credential to a user data publishing website over a cellular data network, and wherein the mobile client application on the short-range wireless enabled cellular phone provides a touch based GUI for the received new-data.

Claim 13 (previously presented): The short-range wireless enabled data capture device of claim 12, 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.

Claim 14 (currently amended): The short-range wireless enabled data capture device of claim 12, wherein the mobile client application for the ~~cryptographically authenticated~~ short-range wireless enabled cellular phone ~~stores the user authentication credential in a non-volatile memory device of the cryptographically authenticated short-range wireless enabled cellular phone, and wherein the mobile client application provides a touch based GUI for the received new-data~~ uses HTTP to send global positioning system information to the user data publishing web service over the cellular data network.

LifeScan, Inc. Ex. 1006
Page 192 of 353
IPR2025-00102

Remarks

The pending claims

Claims 1-9 and 12-14 are currently pending. Reconsideration and allowance of the pending claims is respectfully requested.

Summary of the Office Action

Claim Rejections 35 U.S.C. 112

Claims 1-14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. More specifically, the applicant fails to sufficiently point out or describe: cellular phone remains paired after storing the created new-data; a user authentication credential to a user data publishing website over the cellular data network; 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. The specification of this application under examination does not contain subject matter to implement limitations, as cited in the following claims.
Also, it is not apparent how "remains paired", "a user authentication credential to a user data publishing website over the cellular data network" as recited in claims 1, 4 is determined.

Specification Objection

The disclosure is objected to because of the following informalities: Examiner has reviewed the specification of this application under examination and could not find support for the additional limitations as claimed "remains paired", "a user authentication

LifeScan, Inc. Ex. 1006
Page 193 of 353
IPR2025-00102

credential to a user data publishing website over the cellular data network" "use HTTP to send global positioning system information to the user data publishing website over the cellular data network". Appropriate correction is required.

Claim Rejections - 35 USC § 112

Claims 1-14 are rejected under 112, second paragraph as being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention.

Claim Rejections 35 U.S.C. 103

Claim 1-14 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778.

Amendments to the claims

Claims 1, 3-4, 6-8 and 12 and 14 are currently amended; claims 2, 5, 7, 9 and 13 remain as previously presented; claims 10-11 are cancelled. Applicant respectfully submits that the amendments to the claims do not add any new subject matter.

Support for claim amendments

Support for the amendment: "*wherein the 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, 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 and the user authentication credential to a user data publishing website*** *over a cellular data network*" in claim 1 is found in:

LifeScan, Inc. Ex. 1006
Page 194 of 353
IPR2025-00102

(a) Point No. 2 of "*CROSS REFERENCE TO RELATED APPLICATIONS*" in the originally filed application, which states as follows: "*The following patent application is* ***incorporated herein in its entirety****: US Non-provisional patent application serial number 11/901,802, titled "Online Publishing of Multimedia Content", filed on September 19, 2007 in the United States Patent and Trademark Office." USPTO Publication No. 2008/0103906 A1 is the published application of US Non-provisional patent application serial number 11/901,802. US Non-provisional patent application serial number* ***11/901,802*** *is attached to the response to previously submitted response to non-final office action as* ***Exhibit A*** *and USPTO Publication No.* ***2008/0103906 A1*** *is attached to the previously submitted response to non-final office action as* ***Exhibit B****; see also link: https://patentimages.storage.googleapis.com/1f/06/a0/32f9a69fbef2a6/US20080103906A.pdf."*

(b) **FIG. 4** of **Exhibit B** (reproduced below) Elements **407** and **410**

LifeScan, Inc. Ex. 1006
Page 195 of 353
IPR2025-00102

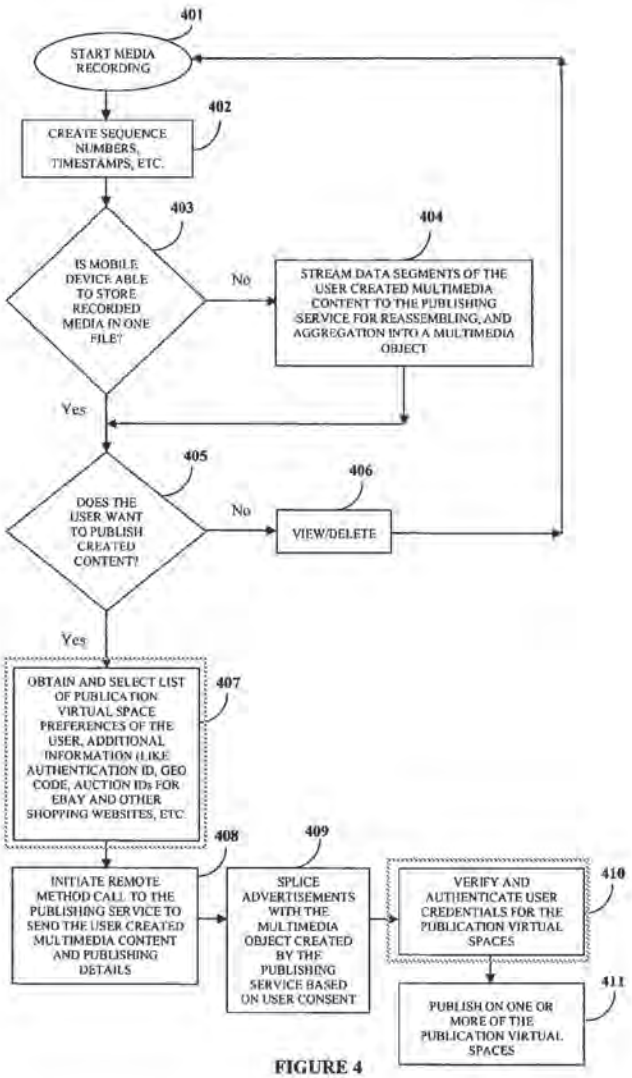


FIGURE 4

(c) Paragraph [0028] of **Exhibit B**, which states: "*The **user 201 may also set preferences on the mobile device**. The **preferences set** by the user **201** 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. These **user preferences are transferred to the publishing service 204.**"*

(d) Paragraph [0037] of **Exhibit B**, which states: "*The **multimedia object is transferred with the user authentication credentials** to the publication virtual spaces **205**. The **user 201 is authenticated** before publishing the user created multimedia content on the chosen publication virtual spaces **205**.*"

(e) Paragraph [0047] of **Exhibit B**, which states: "*Additional information such as the list of the user preferences of the publication virtual spaces **205**, **authentication identification**, user preferences, default settings, manually entered geographical codes, and auction identifiers for eBay® and other shopping websites are selected **407** and **transferred along with the user created multimedia content to the publishing service***".

(f) Paragraph [0049] of **Exhibit B**, which states: "*The multimedia object is transferred to the front end service **204** b of the publishing service **204** from the back end service **204** c. The front end service **204** b associates the multimedia object with the user preferences stored in the database **204** a, **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**.*"

(g) **FIG. 2 Element 202e** of applicant's originally filed application, reproduced below:

LifeScan, Inc. Ex. 1006
Page 197 of 353
IPR2025-00102

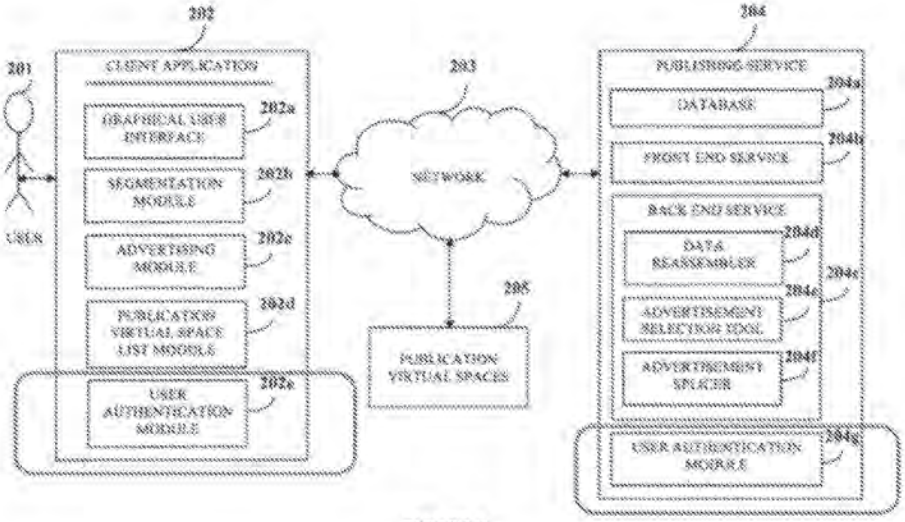


FIGURE 2

2

See also paragraph [0026] of **Exhibit B**, which states: "*When the user **201** starts the client application **202** on the **mobile device**, the user **201** may be authenticated by the user authentication module **202e**,*" claim 16 of Exhibit B, which recites: "*The method of claim 1, wherein the publication virtual spaces are configured by the user and said configuration is **stored on the mobile device**.*" and claim 29 of Exhibit B, which recites: "*The system of claim 21, wherein the **client application** comprises a first user authentication module for **authenticating the user** to publish the user created multimedia content.*"

(h) Paragraph [0023] of **Exhibit B**, which states: "*The **user preferences** may comprise **authentication credentials**, transaction identification, a 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 a compression rate of the multimedia content. **The user 201 stores these preferences** during registration with the publishing service **204**.*"

17

LifeScan, Inc. Ex. 1006
Page 198 of 353
IPR2025-00102

Applicant-Initiated Interview Summary (07 January 2021)

During the interview, an overview of the invention was presented and proposed claim amendments were discussed, which examiner indicated appear to overcome the outstanding rounds of rejection and advancing the prosecution. However, no formal agreement was reached during the interview.

Applicant-Initiated Interview Summary (13 January 2021)

During the interview, examiner suggested filing a response to the final office action incorporating all the points discussed during the interview on 07 January 2021. Furthermore, examiner suggested including proof as to why the contents of USPTO Patent Application No. 11/901,802 (Exhibit A) should be considered as incorporated in its entirety in the present application.

The office action states: "**Claims 1-14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. More specifically, the applicant fails to sufficiently point out or describe: cellular phone remains paired after storing the created new-data; a user authentication credential to a user data publishing website over the cellular data network; 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. The specification of this application under examination does not contain subject matter to implement limitations, as cited in the following claims. Also, it is not apparent how "remains paired", "a user authentication credential to a user data publishing website over the cellular data network" as recited in claims 1, 4 is determined.**"

LifeScan, Inc. Ex. 1006
Page 199 of 353
IPR2025-00102

In response to the above rejection, applicant has removed the recitation "*remains paired*" from the claims. Regarding the other rejections, applicant disagrees and presents the following arguments:

Point No. 2 of "*CROSS REFERENCE TO RELATED APPLICATIONS*" in the originally filed application states as follows: "*The following patent application is* ***incorporated herein in its entirety****: US Non-provisional patent application serial number 11/901,802, titled "Online Publishing of Multimedia Content", filed on September 19, 2007 in the United States Patent and Trademark Office.*" USPTO Publication No. 2008/0103906 A1 is the published application of US Non-provisional patent application serial number 11/901,802. US Non-provisional patent application serial number 11/901,802 is attached to this response as Exhibit A and USPTO Publication No. 2008/0103906 A1 is attached to this response as Exhibit B; see also link: https://patentimages.storage.googleapis.com/1f/06/a0/32f9a69fbef2a6/US20080103906A1.pdf.

Applicant thanks the examiner for the interviews on 07 January 2021 and 13 January 2021, and for commenting on the arguments presented during the interview. In response to the comment that the content of patent application no. 11/901,802 ('802 application, Exhibit A) referenced as an application "incorporated by reference in its entirety" in applicant's pending application no. 16/532,507 ('507 application) on page 2, item 2 of the '507 application, enclosed, cannot be incorporated in the amended claims of the '507 application, applicant conducted some research to determine the provisions for incorporating a prior filed non-provisional as a reference in a later filed non-provisional application. The '802 application (Exhibit A) was also incorporated by reference in its entirety in the parent application (application no. 12/333,303) of the '507 application. In Zenon Environmental Inc v. United States Filter Corporation., Nos. 06-1266, -1267 (Fed. Cir. Nov. 7, 2007), the United States Court of Appeals for the Federal Circuit held that incorporation by reference "***provides a method for integrating material from various documents into a host document . . . by citing such material in a manner that makes***

clear that the material is effectively part of the host document as if it were explicitly contained therein." Cook Biotech Inc. v. Acell, Inc., 460 F.3d 1365, 1376 (Fed. Cir. 2006) (quoting Advanced Display Sys., Inc. v. Kent State Univ., 212 F.3d 1272, 1282 (Fed. Cir. 2000))".

Furthermore, in Paice LLC v. Ford Motor Co., 2018 WL 651366 (Fed. Cir. Feb. 1, 2018), Paice's U.S. Patent No. 7,237,634 ("the '634 patent") claimed priority to U.S. patent application no. 09/264,817 ("the '817 application"). A U.S. Patent no. 5,343,970 was incorporated into the '817 application: with the following paragraph:

"This application discloses a number of improvements over and enhancements to the hybrid vehicles disclosed in the inventor's U.S. Pat. No. 5,343,970 ("the '970 patent"), which is incorporated herein by this reference. Where differences are not mentioned, it is to be understood that the specifics of the vehicle design shown in the '970 patent are applicable to the vehicles shown herein as well."

The Federal Circuit noted that the first sentence above broadly and unambiguously states that '970 patent is, without qualification, incorporated into the '817 application. The Federal Circuit held that the second sentence has no bearing on the extent of incorporation, and merely states that the features disclosed by '970 patent apply to vehicles described as the invention in the '817 application, except if the specification mentions otherwise. Citing *Modine Mfg. Co. v. U.S. Int'l Trade Comm'n*, 75 F.3d 1545 (Fed. Cir. 1996), the Federal Circuit stated that "*[t]he applicability of a document's disclosed features and the incorporation of the document itself are distinct concepts, and one does not imply the other*." In summary, the Federal Circuit held that '970 patent is incorporated into the '817 in its entirety.

In view of the above two Federal circuit decisions, applicant submits that the '802 application (application no. 11/901,802, Exhibit A) is incorporated by reference in its entirety in the '507 application (application no. 16/532,507).

LifeScan, Inc. Ex. 1006
Page 201 of 353
IPR2025-00102

Furthermore, 37 CFR 1.57 (pre-PLT) – Incorporation by Reference, which is applicable to applications filed before December 18, 2013, provides:

> a) Subject to the conditions and requirements of this paragraph, if all or a portion of the specification or drawing(s) is inadvertently omitted from an application, but the application contains a claim …… under §1.78 for the benefit of a prior-filed provisional, non-provisional, or international application, that was present on the filing date of the application, and the inadvertently omitted portion of the specification or drawing(s) is completely contained in the prior-filed application, the claim under ……. §1.78 shall also be considered an incorporation by reference of the prior-filed application as to the inadvertently omitted portion of the specification or drawing(s).
>
> > (1) The application must be amended to include the inadvertently omitted portion of the specification or drawing(s) within any time period set by the Office, but in no case later than the close of prosecution as defined by § 1.114(b), or abandonment of the application, whichever occurs earlier. The applicant is also required to:
> >
> > > (i) Supply a copy of the prior-filed application, except where the prior-filed application is an application filed under 35 U.S.C. 111;
> > >
> > > (ii) Supply an English language translation of any prior-filed application that is in a language other than English; and
> > >
> > > (iii) Identify where the inadvertently omitted portion of the specification or drawings can be found in the prior-filed application.

LifeScan, Inc. Ex. 1006
Page 202 of 353
IPR2025-00102

Applicant submits that the requirements under 37 CFR 1.57(a) were fulfilled by pending application no. 16/532,507 ('507 application), when the '507 application was filed.

At the time of filing, the '507 application recited on page 2, item 2 of the application that the prior filed application no. 11/901,802 ('802 application, Exhibit A) is incorporated in its entirety in the '507 application.

The '802 application (Exhibit A) was pending, and not abandoned, at the time of filing of the '507 application.

37 CFR 1.57(a)(1)(i) and 37 CFR 1.57(a)(1)(ii) are not applicable to the '802 application (Exhibit A), and since the '802 application (Exhibit A) was incorporated by reference in its entirety in the '507 application, 37 CFR 1.57(a)(1)(iii) is satisfied.

Enclosed: (a) Copy of pages 1 and 2 of the specification of pending application no. 16/532,507 ('507 application).

Page Nos. 5, 7, 9 and Figure 2 and Figure 4 of US Non-provisional patent application serial number 11/901,802 (Exhibit A) reproduced below disclose that the client application is *having and sending* "*authentication credentials*" and "*global positioning system geographical codes*" to the publishing website. The corresponding sections in Exhibit B are:

Extract from Page 9 of Exhibit A = Paragraph [0028] in Exhibit B.
Extract from Page 5 of Exhibit A = Paragraph [0018] in Exhibit B.
Extract from Page 7 of Exhibit A = Paragraph [0023] in Exhibit B.

LifeScan, Inc. Ex. 1006
Page 203 of 353
IPR2025-00102

Before the recording begins, the user **201** may change the default publication location, and select the publication virtual spaces **205** for the user created multimedia content on the mobile device. The user **201** may also change the quality of the media before recording the message. For example, if compression is available, the user **201** may change the compression rate, and also change both the transfer speed and message quality. 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, 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. These user preferences are transferred to the publishing service **204**.

Page 9

The method disclosed herein further provides **103** the publishing service **204** comprising a front end service **204b** and a back end service **204c**. The client application **202** interacts with the publishing service **204** to determine the preferred websites or publication virtual spaces **205** of the user **201** for publishing the user created multimedia content. The user **201** may select one or more publication virtual spaces **205** using the client application **202**, as a preferred destination for publishing the user created multimedia content. The client application **202** communicates the user publishing information including the user preferences of the publication virtual spaces **205** to the front end service **204b**. In one embodiment, the publication virtual spaces **205** may be selected on the website of the publishing service **204**. The method disclosed herein provides a protocol for synchronizing **104** user publishing information between the client application **202** and the publishing service **204**. The user publishing information includes user preferences of the publication virtual spaces **205**. The user created multimedia content is received by the front end service **204b** of the publishing service **204** from the client application **202** and then transferred **105** to the back end service **204c** of the publishing service **204**.

Page 5

Furthermore, "Authentication credentials" or "credentials for user authentication" or just "credentials" are mentioned **5** times in the US Non-provisional patent application serial number 11/901,802 (Exhibit A) on pages 7, 9, 12, 13 and in FIGURE 4.

The multimedia object is then transferred **107** from the back end service **204c** to the front end service **204b**. The multimedia object is published **108** by the front end service **204b** according to the user preferences on one or more publication virtual spaces **205** via the network **203**. The user preferences may comprise authentication credentials, transaction identification, a 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 a compression rate of the multimedia content. The user **201** stores these preferences during registration with the publishing service **204**. The publishing service **204** may also collect viewing information each time the multimedia object is viewed on the publication virtual spaces **205**. The viewing information is used to generate advertising statistics. The multimedia object may be published by a single input action of the user **201**. 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, a voice command, or a turn of a scroll wheel on the mobile device.

Page 7

LifeScan, Inc. Ex. 1006
Page 205 of 353
IPR2025-00102

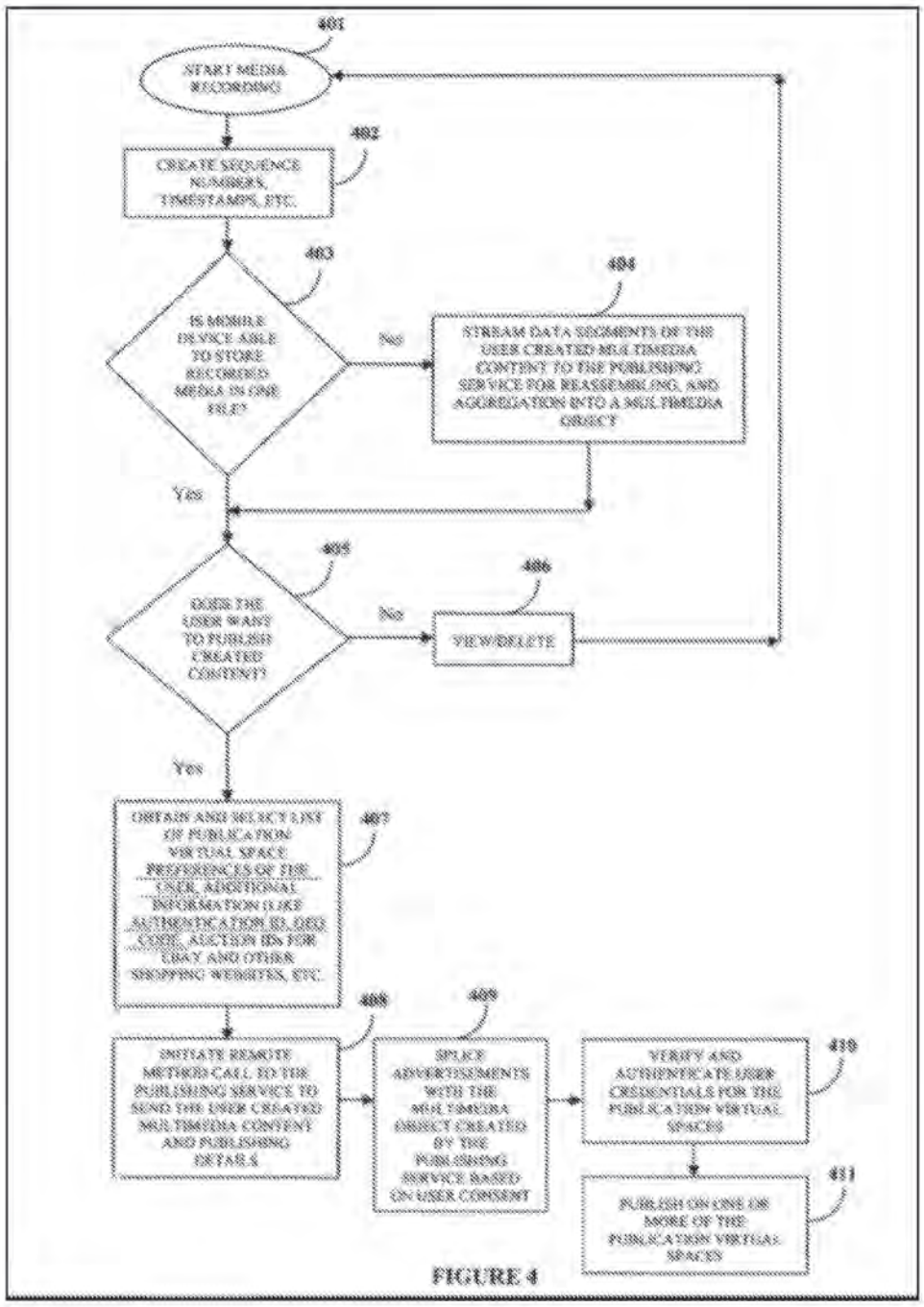


FIGURE 4

Furthermore, "global positioning system geographical codes" is mentioned **twice** in the U.S. No. 11/901,802 (Exhibit A) on **page 7 and page 9.**

Furthermore, "Authentication" as a module is present on the client application and the publishing service as shown in FIGURE 2 of U.S. No. 11/901,802 (Exhibit A) as highlighted below.

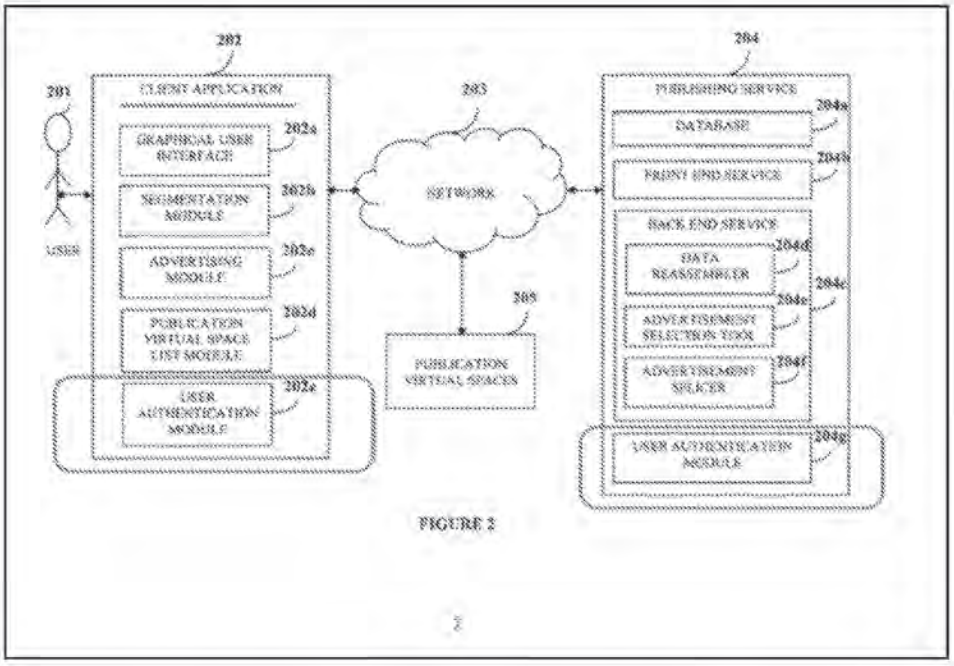


FIGURE 2

Furthermore, "Authentication" as a process step being performed in the state machine is explained in FIGURE 4 of U.S. No. 11/901,802 (Exhibit A) as highlighted above.

Applicant has amended claims 1, 4, 8 and 12, and submits that the amended claims do not contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention.

Applicant therefore respectfully requests that the rejection of claim 1 under 35 U.S.C. 112, first paragraph be reconsidered and withdrawn.

LifeScan, Inc. Ex. 1006
Page 207 of 353
IPR2025-00102

Claims 4, 8 and 12 are analogous to claim 1. Applicant therefore respectfully requests that the rejection of claims 4, 8 and 12 under 35 U.S.C. 112, first paragraph be reconsidered and withdrawn.

Claims 2-3 are dependent on claim 1. Claims 5-7 are dependent on claim 4. Claim 9 is dependent on claim 8. Claims 13-14 are dependent on claim 12. Applicant therefore respectfully requests that the rejection of claims 2-3, 5-7, 9 and 13-14 under 35 U.S.C. 112, first paragraph be reconsidered and withdrawn.

Claims 10-11 are cancelled. Therefore, the rejection of claims 10-11 is moot.

The office action further states: "**The disclosure is objected to because of the following informalities: Examiner has reviewed the specification of this application under examination and could not find support for the additional limitations as claimed "remains paired", "a user authentication credential to a user data publishing website over the cellular data network" "use HTTP to send global positioning system information to the user data publishing website over the cellular data network". Appropriate correction is required.**"

In response to the above rejection, applicant has removed the recitation "*remains paired*" from the claims. Regarding the other rejections, applicant disagrees and presents the following arguments:

Point No. 2 of "*CROSS REFERENCE TO RELATED APPLICATIONS*" in the originally filed application states as follows: "*The following patent application is **incorporated herein in its entirety**: US Non-provisional patent application serial number 11/901,802, titled "Online Publishing of Multimedia Content", filed on September 19, 2007 in the United States Patent and Trademark Office.*" USPTO Publication No. 2008/0103906 A1 is the published application of US Non-provisional patent application serial number 11/901,802. US Non-provisional patent application serial number

LifeScan, Inc. Ex. 1006
Page 208 of 353
IPR2025-00102

11/901,802 is attached to this response as Exhibit A and USPTO Publication No. 2008/0103906 A1 is attached to this response as Exhibit B.

In response to the comment that the content of patent application no. 11/901,802 ('802 application, Exhibit A) referenced as an application "incorporated by reference in its entirety" in applicant's pending application no. 16/532,507 ('507 application) on page 2, item 2 of the '507 application, enclosed, cannot be incorporated in the amended claims of the '507 application, applicant conducted some research to determine the provisions for incorporating a prior filed non-provisional as a reference in a later filed non-provisional application. The '802 application (Exhibit A) was also incorporated by reference in its entirety in the parent application (application no. 12/333,303) of the '507 application. In Zenon Environmental Inc v. United States Filter Corporation., Nos. 06-1266, -1267 (Fed. Cir. Nov. 7, 2007), the United States Court of Appeals for the Federal Circuit held that incorporation by reference "***provides a method for integrating material from various documents into a host document . . . by citing such material in a manner that makes clear that the material is effectively part of the host document as if it were explicitly contained therein***." Cook Biotech Inc. v. Acell, Inc., 460 F.3d 1365, 1376 (Fed. Cir. 2006) (quoting Advanced Display Sys., Inc. v. Kent State Univ., 212 F.3d 1272, 1282 (Fed. Cir. 2000))".

Furthermore, in Paice LLC v. Ford Motor Co., 2018 WL 651366 (Fed. Cir. Feb. 1, 2018), Paice's U.S. Patent No. 7,237,634 ("the '634 patent") claimed priority to U.S. patent application no. 09/264,817 ("the '817 application"). A U.S. Patent no. 5,343,970 was incorporated into the '817 application: with the following paragraph:

"This application discloses a number of improvements over and enhancements to the hybrid vehicles disclosed in the inventor's U.S. Pat. No. 5,343,970 ("the '970 patent"), which is incorporated herein by this reference. Where differences are not mentioned, it is to be understood that the specifics of the vehicle design shown in the '970 patent are applicable to the vehicles shown herein as well."

The Federal Circuit noted that the first sentence above broadly and unambiguously states that '970 patent is, without qualification, incorporated into the '817 application. The Federal Circuit held that the second sentence has no bearing on the extent of incorporation, and merely states that the features disclosed by '970 patent apply to vehicles described as the invention in the '817 application, except if the specification mentions otherwise. Citing *Modine Mfg. Co. v. U.S. Int'l Trade Comm'n*, 75 F.3d 1545 (Fed. Cir. 1996), the Federal Circuit stated that "*[t]he applicability of a document's disclosed features and the incorporation of the document itself are distinct concepts, and one does not imply the other*." In summary, the Federal Circuit held that '970 patent is incorporated into the '817 in its entirety.

In view of the above two Federal circuit decisions, applicant submits that the '802 application (application no. 11/901,802, Exhibit A) is incorporated by reference in its entirety in the '507 application (application no. 16/532,507).

Furthermore, 37 CFR 1.57 (pre-PLT) – Incorporation by Reference, which is applicable to applications filed before December 18, 2013, provides:

> a) Subject to the conditions and requirements of this paragraph, if all or a portion of the specification or drawing(s) is inadvertently omitted from an application, but the application contains a claim ..... under §1.78 for the benefit of a prior-filed provisional, non-provisional, or international application, that was present on the filing date of the application, and the inadvertently omitted portion of the specification or drawing(s) is completely contained in the prior-filed application, the claim under ..... §1.78 shall also be considered an incorporation by reference of the prior-filed application as to the inadvertently omitted portion of the specification or drawing(s).
>
> (2) The application must be amended to include the inadvertently omitted portion of the specification or drawing(s) within any time period set by the Office, but in no case later than the close of prosecution as defined by § 1.114(b), or

LifeScan, Inc. Ex. 1006
Page 210 of 353
IPR2025-00102

abandonment of the application, whichever occurs earlier. The applicant is also required to:

> (i) Supply a copy of the prior-filed application, except where the prior-filed application is an application filed under 35 U.S.C. 111;
>
> (ii) Supply an English language translation of any prior-filed application that is in a language other than English; and
>
> (iii) Identify where the inadvertently omitted portion of the specification or drawings can be found in the prior-filed application.

Applicant submits that the requirements under 37 CFR 1.57(a) were fulfilled by pending application no. 16/532,507 ('507 application), when the '507 application was filed.

At the time of filing, the '507 application recited on page 2, item 2 of the application that the prior filed application no. 11/901,802 ('802 application, Exhibit A) is incorporated in its entirety in the '507 application.

The '802 application (Exhibit A) was pending, and not abandoned, at the time of filing of the '507 application.

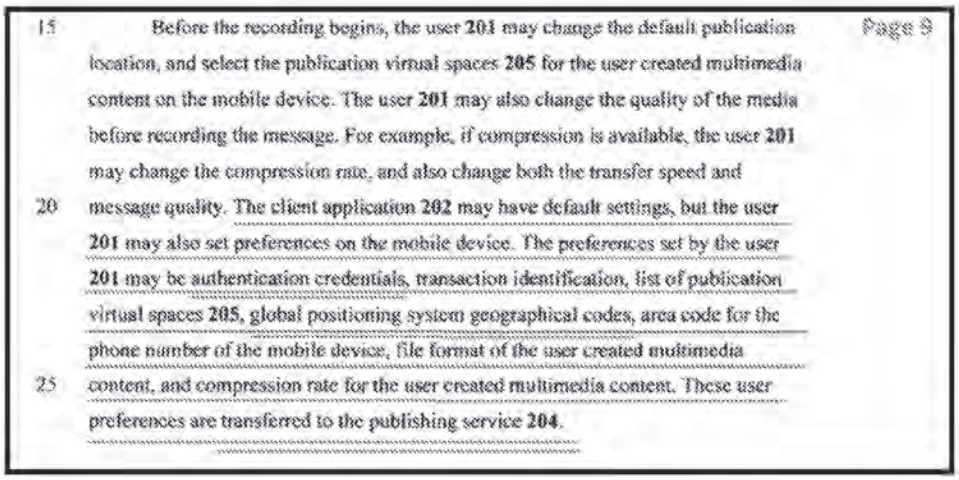
37 CFR 1.57(a)(1)(i) and 37 CFR 1.57(a)(1)(ii) are not applicable to the '802 application (Exhibit A), and since the '802 application (Exhibit A) was incorporated by reference in its entirety in the '507 application, 37 CFR 1.57(a)(1)(iii) is satisfied.

Enclosed: (a) Copy of pages 1 and 2 of the specification of pending application no. 16/532,507 ('507 application).

LifeScan, Inc. Ex. 1006
Page 211 of 353
IPR2025-00102

Page Nos. 5, 7, 9 and Figure 2 and Figure 4 of US Non-provisional patent application serial number 11/901,802 (Exhibit A) reproduced below disclose that the client application is *having and sending* "*authentication credentials*" and "*global positioning system geographical codes*" to the publishing website. The corresponding sections in Exhibit B are:

Extract from Page 9 of Exhibit A = Paragraph [0028] in Exhibit B.
Extract from Page 5 of Exhibit A = Paragraph [0018] in Exhibit B.
Extract from Page 7 of Exhibit A = Paragraph [0023] in Exhibit B.



Before the recording begins, the user **201** may change the default publication location, and select the publication virtual spaces **205** for the user created multimedia content on the mobile device. The user **201** may also change the quality of the media before recording the message. For example, if compression is available, the user **201** may change the compression rate, and also change both the transfer speed and message quality. 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, 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. These user preferences are transferred to the publishing service **204**.

Page 9

The method disclosed herein further provides **103** the publishing service **204** comprising a front end service **204b** and a back end service **204c**. The client application **202** interacts with the publishing service **204** to determine the preferred websites or publication virtual spaces **205** of the user **201** for publishing the user created multimedia content. The user **201** may select one or more publication virtual spaces **205** using the client application **202**, as a preferred destination for publishing the user created multimedia content. The client application **202** communicates the user publishing information including the user preferences of the publication virtual spaces **205** to the front end service **204b**. In one embodiment, the publication virtual spaces **205** may be selected on the website of the publishing service **204**. The method disclosed herein provides a protocol for synchronizing **104** user publishing information between the client application **202** and the publishing service **204**. The user publishing information includes user preferences of the publication virtual spaces **205**. The user created multimedia content is received by the front end service **204b** of the publishing service **204** from the client application **202** and then transferred **105** to the back end service **204c** of the publishing service **204**.

Page 5

Furthermore, "Authentication credentials" or "credentials for user authentication" or just "credentials" are mentioned **5** times in the US Non-provisional patent application serial number 11/901,802 (Exhibit A) on pages 7, 9, 12, 13 and in FIGURE 4.

The multimedia object is then transferred **107** from the back end service **204c** to the front end service **204b**. The multimedia object is published **108** by the front end service **204b** according to the user preferences on one or more publication virtual spaces **205** via the network **203**. The user preferences may comprise authentication credentials, transaction identification, a 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 a compression rate of the multimedia content. The user **201** stores these preferences during registration with the publishing service **204**. The publishing service **204** may also collect viewing information each time the multimedia object is viewed on the publication virtual spaces **205**. The viewing information is used to generate advertising statistics. The multimedia object may be published by a single input action of the user **201**. 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, a voice command, or a turn of a scroll wheel on the mobile device.

Page 7

LifeScan, Inc. Ex. 1006
Page 214 of 353
IPR2025-00102

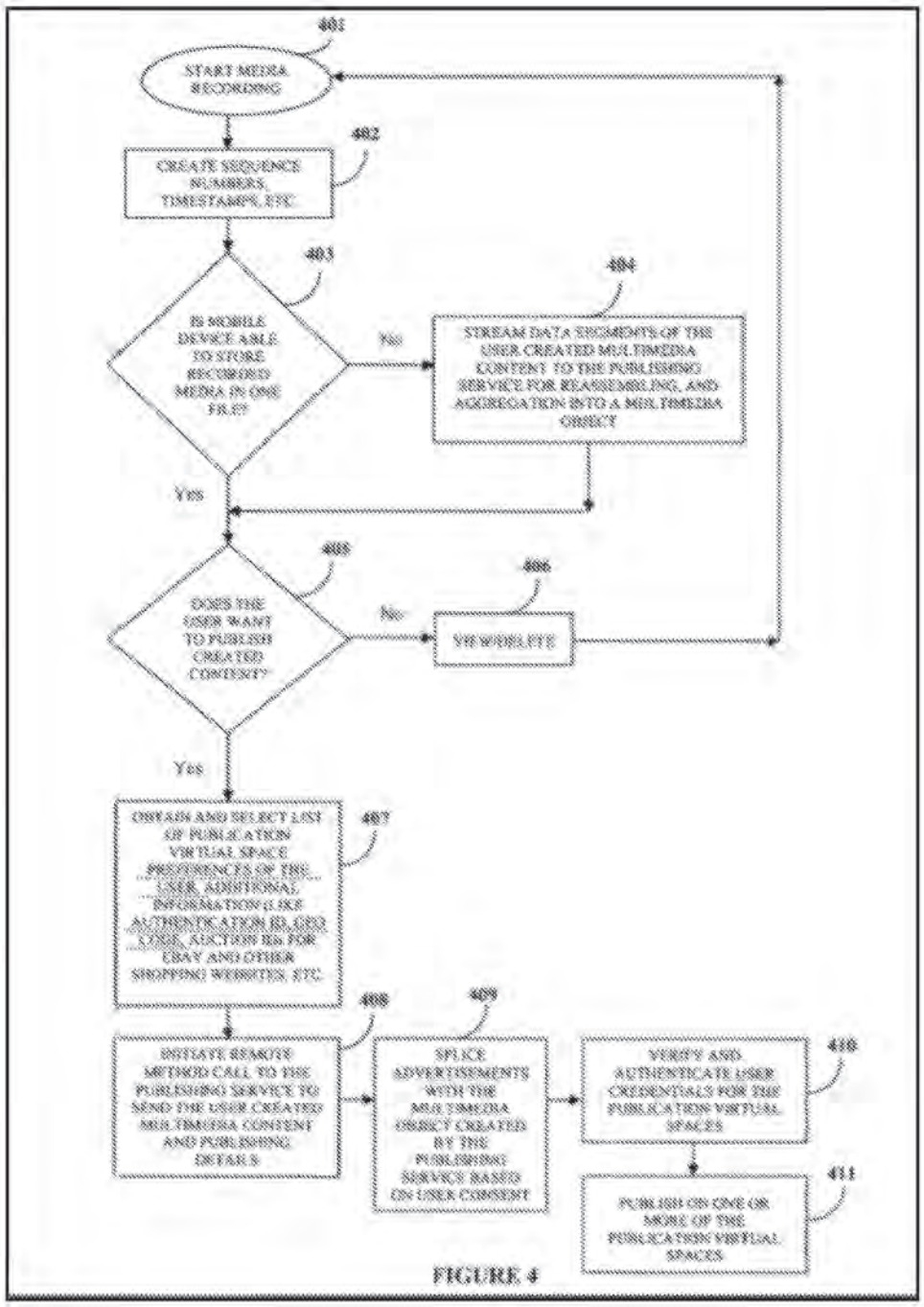
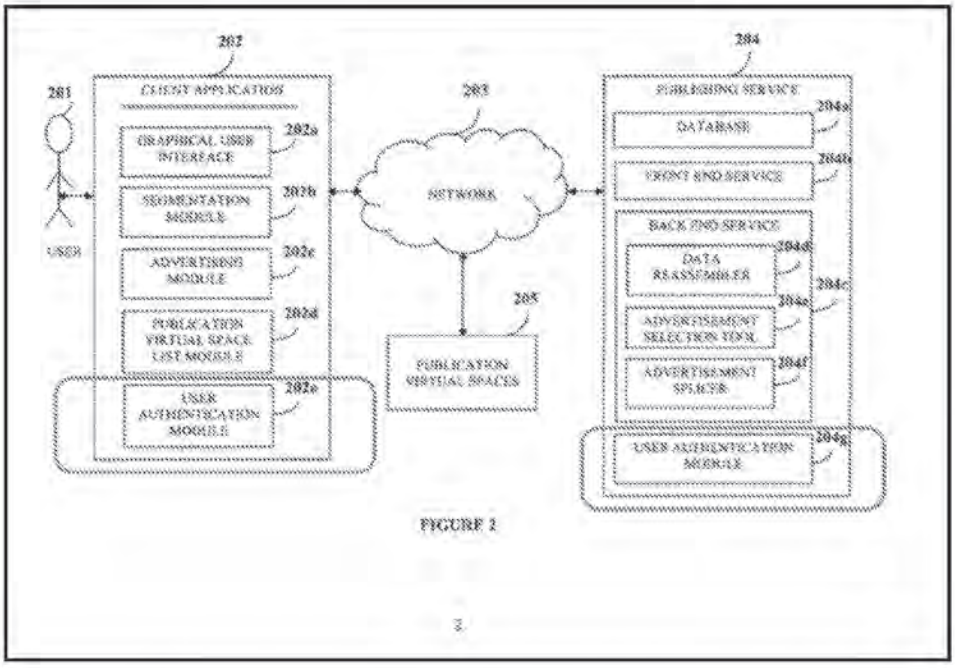


FIGURE 4

Furthermore, "global positioning system geographical codes" is mentioned **twice** in the U.S. No. 11/901,802 (Exhibit A) on page 7 and page 9.

Furthermore, "Authentication" as a module is present on the client application and the publishing service as shown in FIGURE 2 of U.S. No. 11/901,802 (Exhibit A) as highlighted below.



Furthermore, "Authentication" as a process step being performed in the state machine is explained in FIGURE 4 of U.S. No. 11/901,802 (Exhibit A) as highlighted above.

Applicant has amended claims 1, 4, 8 and 12, and submits that the amended claims do not contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention.

LifeScan, Inc. Ex. 1006
Page 216 of 353
IPR2025-00102

Applicant therefore respectfully requests that the objection to the specification be reconsidered and withdrawn.

The office action further states: "**Claims 1-14 are rejected under 112, second paragraph as being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention.**"

Applicant disagrees with the above rejection and presents the following arguments:

Point No. 2 of "*CROSS REFERENCE TO RELATED APPLICATIONS*" in the originally filed application states as follows: "*The following patent application is* ***incorporated herein in its entirety****: US Non-provisional patent application serial number 11/901,802, titled "Online Publishing of Multimedia Content", filed on September 19, 2007 in the United States Patent and Trademark Office.*" USPTO Publication No. 2008/0103906 A1 is the published application of US Non-provisional patent application serial number 11/901,802. US Non-provisional patent application serial number 11/901,802 is attached to this response as Exhibit A and USPTO Publication No. 2008/0103906 A1 is attached to this response as Exhibit B.

In response to the comment that the content of patent application no. 11/901,802 ('802 application, Exhibit A) referenced as an application "incorporated by reference in its entirety" in applicant's pending application no. 16/532,507 ('507 application) on page 2, item 2 of the '507 application, enclosed, cannot be incorporated in the amended claims of the '507 application, applicant conducted some research to determine the provisions for incorporating a prior filed non-provisional as a reference in a later filed non-provisional application. The '802 application (Exhibit A) was also incorporated by reference in its entirety in the parent application (application no. 12/333,303) of the '507 application. In Zenon Environmental Inc v. United States Filter Corporation., Nos. 06-1266, -1267 (Fed. Cir. Nov. 7, 2007), the United States Court of Appeals for the Federal

LifeScan, Inc. Ex. 1006
Page 217 of 353
IPR2025-00102

Circuit held that incorporation by reference "***provides a method for integrating material from various documents into a host document . . . by citing such material in a manner that makes clear that the material is effectively part of the host document as if it were explicitly contained therein***." Cook Biotech Inc. v. Acell, Inc., 460 F.3d 1365, 1376 (Fed. Cir. 2006) (quoting Advanced Display Sys., Inc. v. Kent State Univ., 212 F.3d 1272, 1282 (Fed. Cir. 2000))".

Furthermore, in Paice LLC v. Ford Motor Co., 2018 WL 651366 (Fed. Cir. Feb. 1, 2018), Paice's U.S. Patent No. 7,237,634 ("the '634 patent") claimed priority to U.S. patent application no. 09/264,817 ("the '817 application"). A U.S. Patent no. 5,343,970 was incorporated into the '817 application: with the following paragraph:

"This application discloses a number of improvements over and enhancements to the hybrid vehicles disclosed in the inventor's U.S. Pat. No. 5,343,970 ("the '970 patent"), which is incorporated herein by this reference. Where differences are not mentioned, it is to be understood that the specifics of the vehicle design shown in the '970 patent are applicable to the vehicles shown herein as well."

The Federal Circuit noted that the first sentence above broadly and unambiguously states that '970 patent is, without qualification, incorporated into the '817 application. The Federal Circuit held that the second sentence has no bearing on the extent of incorporation, and merely states that the features disclosed by '970 patent apply to vehicles described as the invention in the '817 application, except if the specification mentions otherwise. Citing *Modine Mfg. Co. v. U.S. Int'l Trade Comm'n*, 75 F.3d 1545 (Fed. Cir. 1996), the Federal Circuit stated that "*[t]he applicability of a document's disclosed features and the incorporation of the document itself are distinct concepts, and one does not imply the other*." In summary, the Federal Circuit held that '970 patent is incorporated into the '817 in its entirety.

In view of the above two Federal circuit decisions, applicant submits that the '802 application (application no. 11/901,802, Exhibit A) is incorporated by reference in its entirety in the '507 application (application no. 16/532,507).

Furthermore, 37 CFR 1.57 (pre-PLT) – Incorporation by Reference, which is applicable to applications filed before December 18, 2013, provides:

> a) Subject to the conditions and requirements of this paragraph, if all or a portion of the specification or drawing(s) is inadvertently omitted from an application, but the application contains a claim ..... under §1.78 for the benefit of a prior-filed provisional, non-provisional, or international application, that was present on the filing date of the application, and the inadvertently omitted portion of the specification or drawing(s) is completely contained in the prior-filed application, the claim under ..... §1.78 shall also be considered an incorporation by reference of the prior-filed application as to the inadvertently omitted portion of the specification or drawing(s).
>
> (3) The application must be amended to include the inadvertently omitted portion of the specification or drawing(s) within any time period set by the Office, but in no case later than the close of prosecution as defined by § 1.114(b), or abandonment of the application, whichever occurs earlier. The applicant is also required to:
>
> > (i) Supply a copy of the prior-filed application, except where the prior-filed application is an application filed under 35 U.S.C. 111;
> >
> > (ii) Supply an English language translation of any prior-filed application that is in a language other than English; and

LifeScan, Inc. Ex. 1006
Page 219 of 353
IPR2025-00102

(iii) Identify where the inadvertently omitted portion of the specification or drawings can be found in the prior-filed application.

Applicant submits that the requirements under 37 CFR 1.57(a) were fulfilled by pending application no. 16/532,507 ('507 application), when the '507 application was filed.

At the time of filing, the '507 application recited on page 2, item 2 of the application that the prior filed application no. 11/901,802 ('802 application, Exhibit A) is incorporated in its entirety in the '507 application.

The '802 application (Exhibit A) was pending, and not abandoned, at the time of filing of the '507 application.

37 CFR 1.57(a)(1)(i) and 37 CFR 1.57(a)(1)(ii) are not applicable to the '802 application (Exhibit A), and since the '802 application (Exhibit A) was incorporated by reference in its entirety in the '507 application, 37 CFR 1.57(a)(1)(iii) is satisfied.

Enclosed: (a) Copy of pages 1 and 2 of the specification of pending application no. 16/532,507 ('507 application).

Page Nos. 5, 7, 9 and Figure 2 and Figure 4 of US Non-provisional patent application serial number 11/901,802 (Exhibit A) reproduced below disclose that the client application is *having and sending* "*authentication credentials*" and "*global positioning system geographical codes*" to the publishing website. The corresponding sections in Exhibit B are:

Extract from Page 9 of Exhibit A = Paragraph [0028] in Exhibit B.
Extract from Page 5 of Exhibit A = Paragraph [0018] in Exhibit B.
Extract from Page 7 of Exhibit A = Paragraph [0023] in Exhibit B.

Before the recording begins, the user **201** may change the default publication location, and select the publication virtual spaces **205** for the user created multimedia content on the mobile device. The user **201** may also change the quality of the media before recording the message. For example, if compression is available, the user **201** may change the compression rate, and also change both the transfer speed and message quality. 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, 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. These user preferences are transferred to the publishing service **204**.

Page 9

The method disclosed herein further provides **103** the publishing service **204** comprising a front end service **204b** and a back end service **204c**. The client application **202** interacts with the publishing service **204** to determine the preferred websites or publication virtual spaces **205** of the user **201** for publishing the user created multimedia content. The user **201** may select one or more publication virtual spaces **205** using the client application **202**, as a preferred destination for publishing the user created multimedia content. The client application **202** communicates the user publishing information including the user preferences of the publication virtual spaces **205** to the front end service **204b**. In one embodiment, the publication virtual spaces **205** may be selected on the website of the publishing service **204**. The method disclosed herein provides a protocol for synchronizing **104** user publishing information between the client application **202** and the publishing service **204**. The user publishing information includes user preferences of the publication virtual spaces **205**. The user created multimedia content is received by the front end service **204b** of the publishing service **204** from the client application **202** and then transferred **105** to the back end service **204c** of the publishing service **204**.

Page 5

Furthermore, "Authentication credentials" or "credentials for user authentication" or just "credentials" are mentioned **5** times in the US Non-provisional patent application serial number 11/901,802 (Exhibit A) on pages 7, 9, 12, 13 and in FIGURE 4.

The multimedia object is then transferred **107** from the back end service **204c** to the front end service **204b**. The multimedia object is published **108** by the front end service **204b** according to the user preferences on one or more publication virtual spaces **205** via the network **203**. The user preferences may comprise authentication credentials, transaction identification, a 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 a compression rate of the multimedia content. The user **201** stores these preferences during registration with the publishing service **204**. The publishing service **204** may also collect viewing information each time the multimedia object is viewed on the publication virtual spaces **205**. The viewing information is used to generate advertising statistics. The multimedia object may be published by a single input action of the user **201**. 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, a voice command, or a turn of a scroll wheel on the mobile device.

Page 7

LifeScan, Inc. Ex. 1006
Page 222 of 353
IPR2025-00102

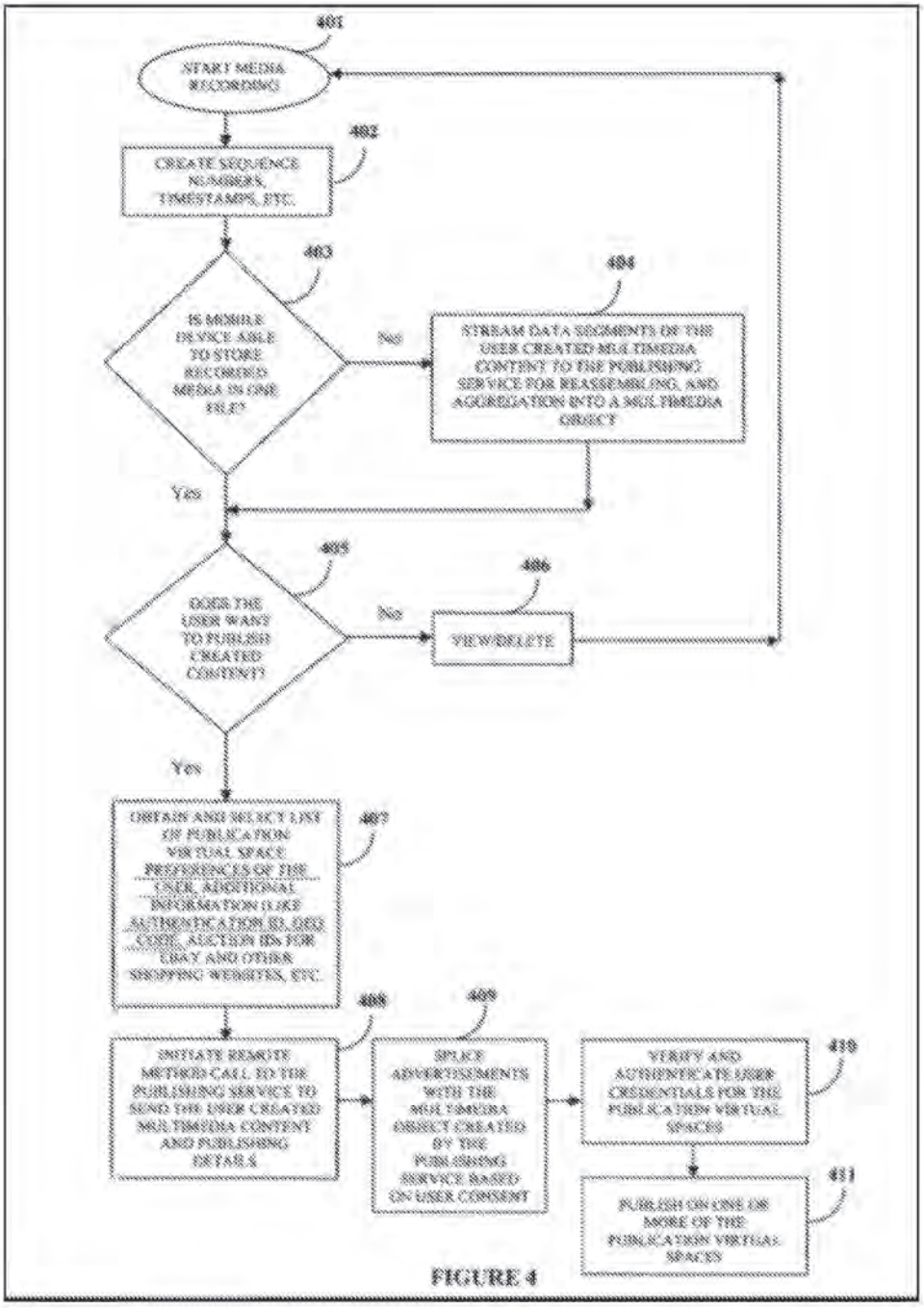


FIGURE 4

Furthermore, "global positioning system geographical codes" is mentioned **twice** in the U.S. No. 11/901,802 (Exhibit A) on page 7 and page 9.

Furthermore, "Authentication" as a module is present on the client application and the publishing service as shown in FIGURE 2 of U.S. No. 11/901,802 (Exhibit A) as highlighted below.

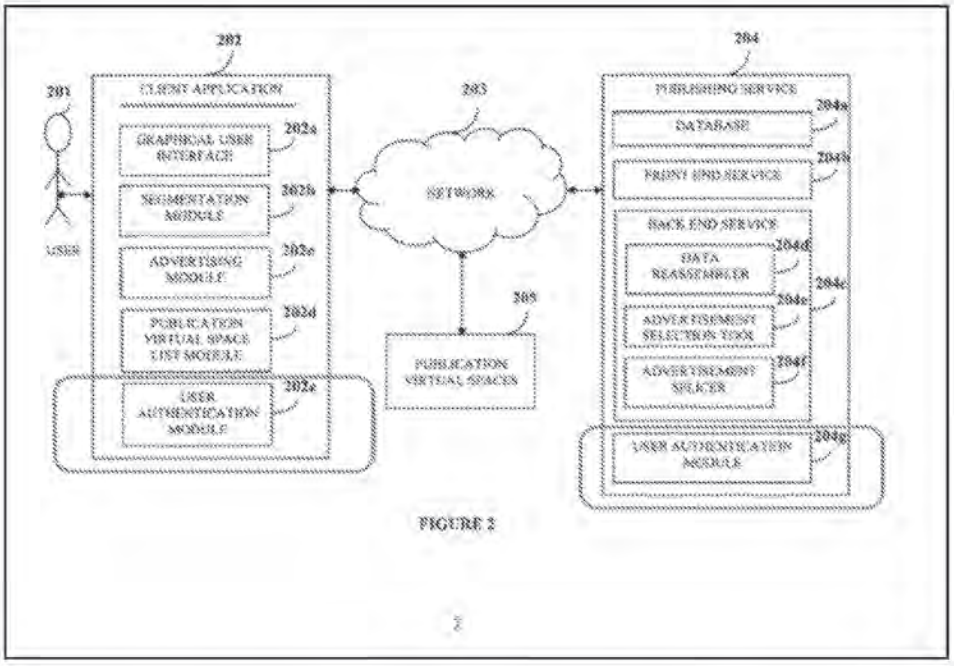


FIGURE 2

Furthermore, "Authentication" as a process step being performed in the state machine is explained in FIGURE 4 of U.S. No. 11/901,802 (Exhibit A) as highlighted above.

Applicant has amended claims 1, 4, 8 and 12, and submits that the amended claims do not contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention.

Applicant therefore respectfully requests that the rejection of claim 1 under 35 U.S.C. 112, second paragraph be reconsidered and withdrawn.

LifeScan, Inc. Ex. 1006
Page 224 of 353
IPR2025-00102

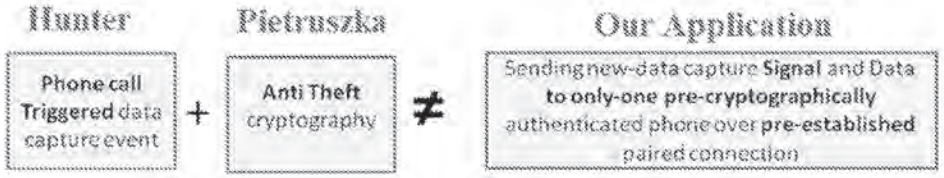
Claims 4, 8 and 12 are analogous to claim 1. Applicant therefore respectfully requests that the rejection of claims 4, 8 and 12 under 35 U.S.C. 112, second paragraph be reconsidered and withdrawn.

Claims 2-3 are dependent on claim 1. Claims 5-7 are dependent on claim 4. Claim 9 is dependent on claim 8. Claims 13-14 are dependent on claim 12. Applicant therefore respectfully requests that the rejection of claims 2-3, 5-7, 9 and 13-14 under 35 U.S.C. 112, second paragraph be reconsidered and withdrawn.

Claims 10-11 are cancelled. Therefore, the rejection of claims 10-11 is moot.

The office action further states: "**Claims 1-14 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778.**"

In response to the above rejection, applicant submits that Hunter, in view of Pietruszka does not teach or suggest all the limitations in claim 1. Furthermore, there is **no motivation** to combine (i) Phone call triggered data capture event of Hunter with (ii) the Anti-Theft Pietruszka teaching.



Arguments

Point#1: **Establishment of <u>non-paired connection</u> (Hunter)**

VS

Establishment of <u>paired</u> short-range Wireless (Applicant)

LifeScan, Inc. Ex. 1006
Page 225 of 353
IPR2025-00102

The office action on page 5 states that Hunter teaches the step of acquiring new-data 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. Applicant disagrees and presents the following arguments.

Hunter prior art does NOT teach pairing or paired connection. There is NO mention of word pair, pairing, paired in Hunter Specification. **Short-range Pairing** and **Paired wireless connection** are terms of short-range wireless technology and have been known and was used in the wireless industry for almost 10 years before the Cellspin patent's priority date of December 2007. Bluetooth wireless standard organization was the first to introduce the term "Bluetooth" at the Blackberry technology consortium in 1998; see Exhibit C, also available at the link: https://web.archive.org/web/20180525083558/https://www.bluetooth.com/about-us/our-history. Furthermore, in 1999, the detailed Bluetooth 1.0 specification with pairing was released; see Exhibit D attached to this response; also available at the link: http://grouper.ieee.org/groups/802/15/Bluetooth/profile_10_b.pdf.

The concept of a paired connection, as established by the **Bluetooth** Special Interest Group (**Bluetooth SIG**), became known and adopted by certain other industry organizations creating short-range wireless technology for device connections, such as WiFi Alliance and Zigbee Forum. In the context of short-range wireless connections, the term "pairing" was adopted by the wireless industry almost 10 years before the Cellspin patent's priority date of December 2007. Drawing from short-range wireless industry's understanding of the term "*paired connection*" / pairing, the **broadest reasonable interpretation** (BRI) of "*paired connection*" as understood by POSITA in Dec 2007, i.e. 10 years after the term was introduced in the wireless lexicon is:

> "bidirectional communications link between devices which provides for encrypted data exchange between the devices, and the communication link can be disconnected and reconnected without having to repeat pairing or authentication."

LifeScan, Inc. Ex. 1006
Page 226 of 353
IPR2025-00102

Because short-range "pairing" is a well-understood term in the art, the applicant followed Federal Court's direction that the **"patent need not teach, and preferably omits, what is well known in the art."** *See McRO, Inc. v. Bandai Namco Games Am. Inc., 959 F.3d 1091, 1102 (Fed. Cir. 2020).* In conformance with this guidance, the applicant cited a version of "pairing" at least 50 times without explicitly defining it. Additionally, while not explicitly defining "pairing," the applicant provided guidance to a POSITA that short-range "pairing" should conform to Bluetooth's conception of the term, which was later adopted when ZigBee and WiFi adopted pairing, making it the only definition applicable to short-range paired wireless connections whether or not a Bluetooth Connection.

Point#2: **Receiving or making Phone call trigger event (Hunter)**

VS

NO such Phone call trigger event (Applicant)

The office action on page 6 states that Hunter teaches the step of acquiring new-data 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. Applicant disagrees and presents the following arguments.

The sequence of events in Hunter is as follows:

(i) Mobile device generates a trigger event or signal in response to a phone call received by the mobile device or a phone call made by the mobile device.

(ii) Send the trigger event or signal from the mobile device to the data capture device.

LifeScan, Inc. Ex. 1006
Page 227 of 353
IPR2025-00102

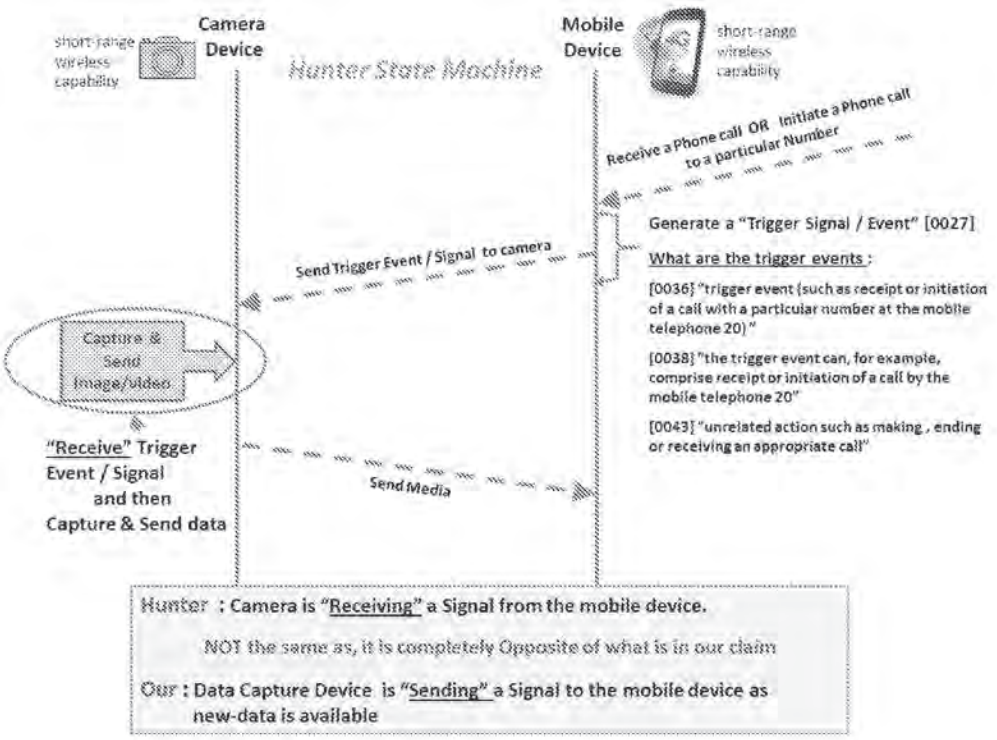
(iii) Only after receipt of the trigger event or signal from the mobile device, the data capture device acquires new-data and transmits the same to the mobile device for onward transfer to a website or web service.

Firstly, in Hunter, there is **NO pairing** of the mobile device by the data capture device. Next, there is NO cryptographic authentication of the mobile device by the data capture device. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be sent to the data capture device.

Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where a data capture device acquires new-data after a short-range paired wireless connection is established with a cellular phone (without any phone call trigger event from the cellular phone to the data capture device).

Next, **in Hunter, the phone call trigger event is sent from the mobile device to the data capture device. This is in direct contrast to applicant's disclosure,** where, after acquiring the new-data, the data capture device sends a notification signal to the mobile device informing the mobile device that it has acquired the new-data.

LifeScan, Inc. Ex. 1006
Page 228 of 353
IPR2025-00102

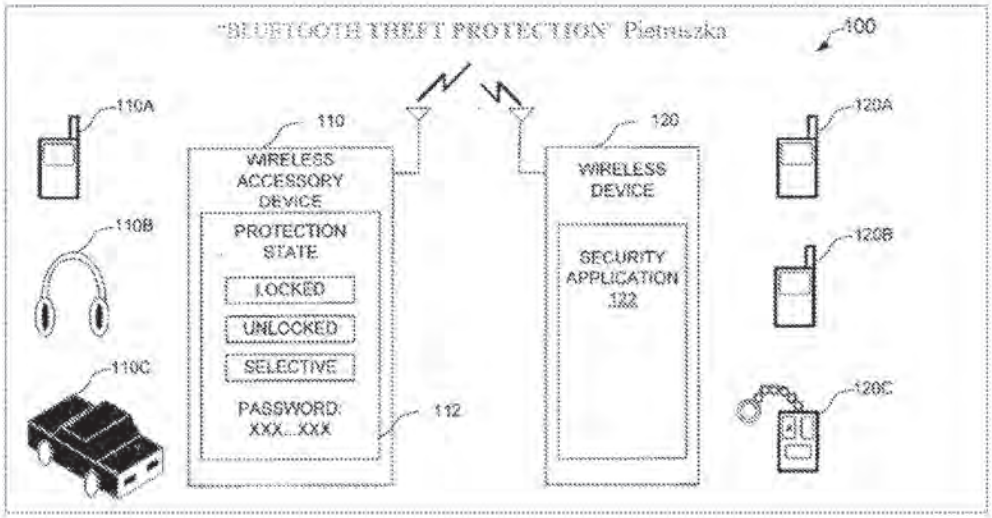


Point#3: Hunter Teaching Away from long lasting paired short-range wireless connection

Hunter is teaching away from the concept of maintaining a long lasting paired Bluetooth wireless connection between the camera and the mobile device (see Hunter paragraph [0009] which states as follows: "*For this reason a permanent connection to the phone is **not appropriate***," and "*It is **not easy** to maintain a voice conversation while interacting with a phone and or a camera to initiate image transfer, for example by attaching a detachable camera as described in EP-A09751342 or by configuring a Bluetooth link between a phone and a camera.*"

Point#4: Anti-Theft Pietruszka Setting based control of cryptographic pairing between devices is NOT relevant in applicant's scenario

LifeScan, Inc. Ex. 1006
Page 229 of 353
IPR2025-00102



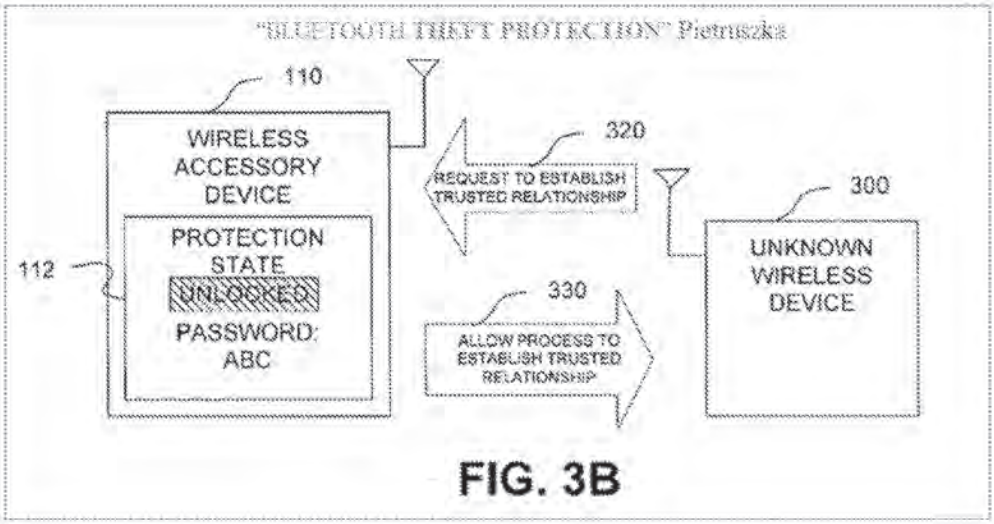


FIG. 3B

Pietruszka ("BLUETOOTH **THEFT PROTECTION**") discloses, *inter alia*, the following:

(a) User pre-selects whether or not a wireless communications device is allowed to establish a cryptographic pairing with a remote device.

LifeScan, Inc. Ex. 1006
Page 230 of 353
IPR2025-00102

(b) Control whether the wireless communications device is able to establish a cryptographic pairing with a remote device **according to the pre-set operational state**; see Pietruszka claim 1, and Paragraph [0005].

Pietruszka teaches mainly a setting-based control of cryptographic pairing between devices and it is not applicable in applicant's scenario. Applicant is NOT using a setting-based control for cryptographic pairing between devices.

Applicant is not implementing any Anti-theft technology. Applicant is not interested in a car or a key fob, or someone else hacking the car to steal it or the car accessories.

Pietruszka **teaches mainly an Anti theft technology and is not applicable in applicant's scenario. Applicant is NOT using pre-set operational state based cryptographic pairing for Anti Theft purposes for car or car accessories.**

Furthermore, in Pietruszka, **car or a key fob is "*NOT* a data capture device" and does not send any data through the mobile phone to the internet.**

In Pietruszka there is **NO** data capture device. **Car or a key fob** device described in Pietruszka is used as a *theft control device*. The **Car or a key fob** device is **NOT capturing any data for transfer through the mobile device.**

Furthermore, in Pietruszka, NO new-data is acquired for sending to the mobile phone after establishing the short-range paired wireless connection. Pietruszka's invention is all about the theft protection based on **pre-set operational state** of the device in its proximity.

Furthermore, there is NO Motivation to combine an anti theft Pietruszka with Hunter to capture data and send data to a website using a cellphone.

LifeScan, Inc. Ex. 1006
Page 231 of 353
IPR2025-00102

In view of above Points 1-4, applicant submits that Hunter, in view of Pietruszka does not teach or suggest the following limitations in amended claim 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, 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;"

> "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;"

Point#5: **Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data.**

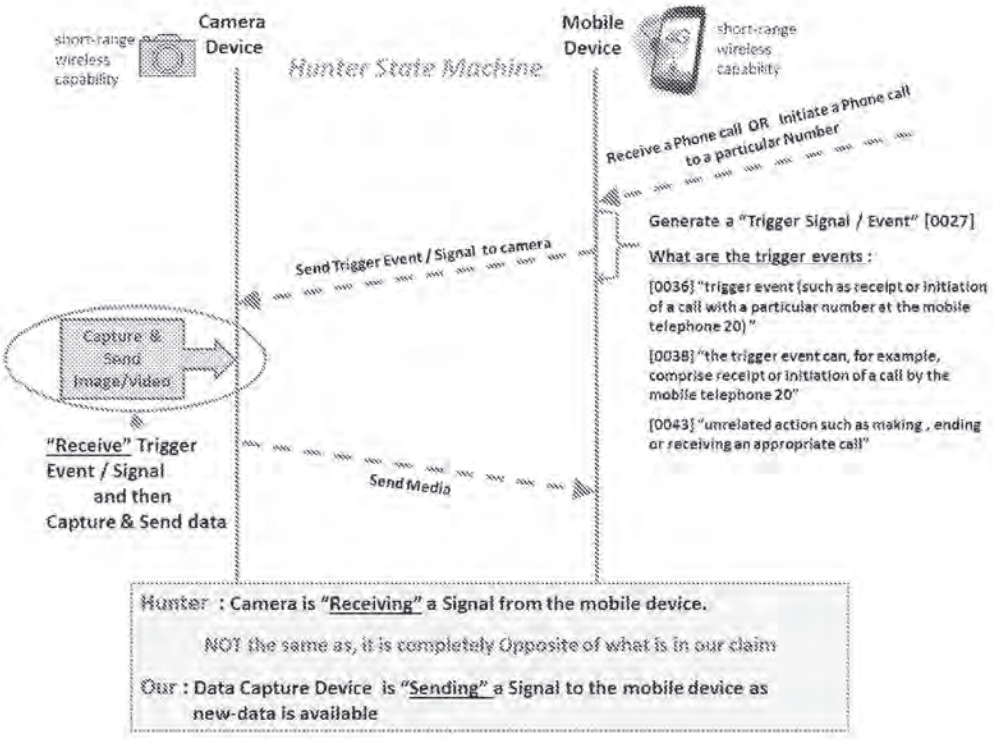
In amended claim 1, applicant discloses that after establishing the paired short-range wireless connection between the data capture device and the cryptographically authenticated short-range wireless enabled cellular phone, and after acquiring new-data, the short-range wireless enabled data capture device sends the event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone.

LifeScan, Inc. Ex. 1006
Page 232 of 353
IPR2025-00102

The office action on page 6 states that paragraph [0013] of Hunter teaches: "*Sending an event notification to a cryptographically authenticated Bluetooth enabled cellular phone*". Applicant disagrees and presents the following arguments.

Paragraph [0013] of Hunter states as follows: "*programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween; transferring images between the camera and the communications device over the wireless link; and transferring said images from the communications device on to a data network through a data network interface.*"

Hunter state machine is again reproduced below to explain paragraph [0013]:



LifeScan, Inc. Ex. 1006
Page 233 of 353
IPR2025-00102

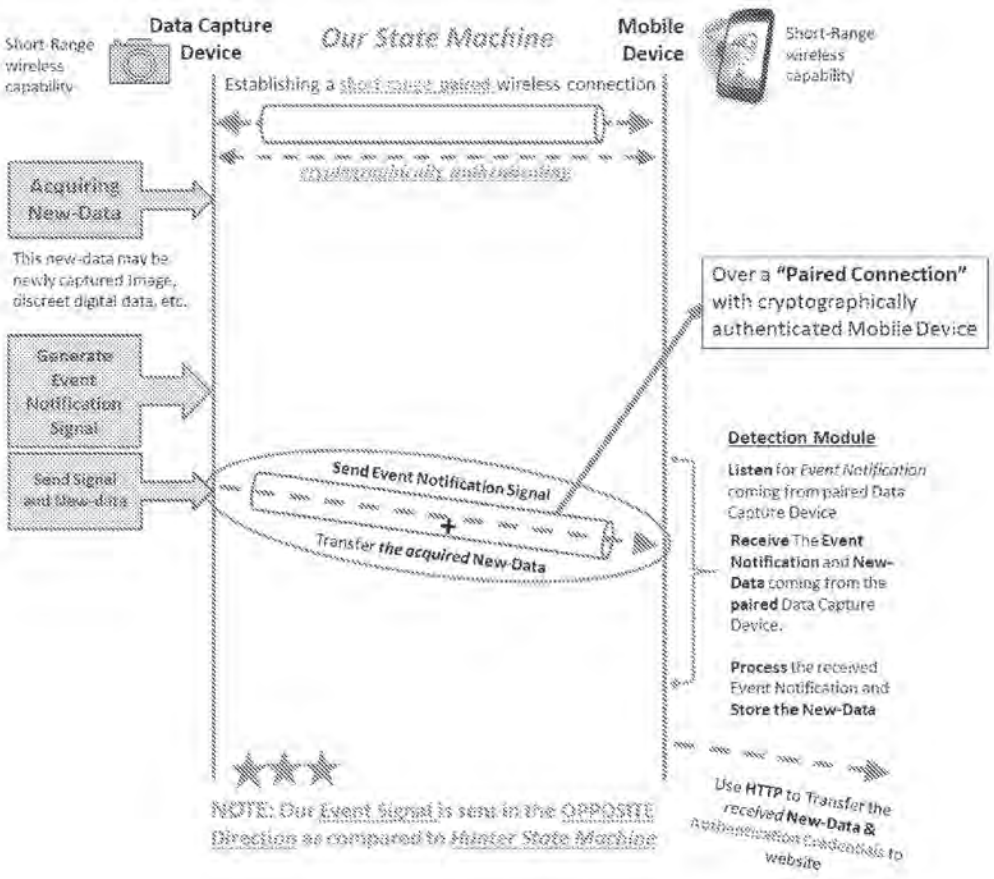
Firstly, in Hunter, there is NO cryptographic authentication of the mobile device by the data capture device before the signal is sent or the data is sent. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be sent to the data capture device.

Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. **This is in direct contrast** to applicant's disclosure where a data capture device acquires new-data after a short-range paired wireless connection is established with a cellular phone (without any phone call trigger event from the cellular phone to the data capture device).

Next, in Hunter, the phone call trigger event is sent from the mobile device to the data capture device. **Event Signal is sent in the opposite direction when compared to the applicants claims. Direction of event signal is in direct contrast to applicant's disclosure,** where, after acquiring the new-data, the data capture device sends a notification signal to the mobile device informing the mobile device that it has acquired the new-data.

In contrast, applicant's state machine is shown below.

LifeScan, Inc. Ex. 1006
Page 234 of 353
IPR2025-00102



Therefore, it is clear that the trigger notification in Hunter is not the same as the event notification in applicant's disclosure. Furthermore, in **Hunter, receipt of a phone call or an outgoing phone call is required** for the mobile device to generate the trigger event to be sent to the camera. Furthermore, in Hunter, the camera acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where the data capture device acquires new-data immediately after the paired short-range wireless connection is established (without any phone call trigger event from the mobile device). Furthermore, in Hunter, the trigger event or signal is sent from the mobile device to the camera, and image capture occurs after receiving the trigger event. **This is in direct contrast to applicant's disclosure.**

LifeScan, Inc. Ex. 1006
Page 235 of 353
IPR2025-00102

where, after acquiring the new-data, the data capture device sends the notification signal to the mobile device informing the mobile device that it has acquired the new-data.

Point#6: Phone call Trigger event in Hunter (see paragraphs [0036], [0038], [0043]) over NON paired connection

As illustrated before, in Hunter, there is no cryptographic authentication of the mobile device by the camera. Furthermore, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate the trigger event or signal to be sent to the camera. Furthermore, in Hunter, the camera acquires the new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where the data capture device acquires the new-data immediately after a paired short-range wireless connection is established (without any phone call trigger event from the mobile device). Furthermore, in Hunter, the phone call trigger event or signal is sent from the mobile device to the camera. This is in direct contrast to applicant's disclosure, where, after acquiring the new-data, the data capture device sends the notification signal and the acquired new-data to the mobile device.

Point#7: Use HTTP to transfer new-data and a user authentication credential to website

In applicant's invention, the cellular phone uses HTTP to transfer new-data and a user authentication credential to website. Neither Hunter nor Pietruszka teach or suggest the use of HTTP to transfer the new-data and the user authentication credential to the website.

In view of above Points 5-7, applicant submits that Hunter, in view of Pietruszka does not teach or suggest the following limitation in amended claim 1:

"said processor further configured to send an event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled

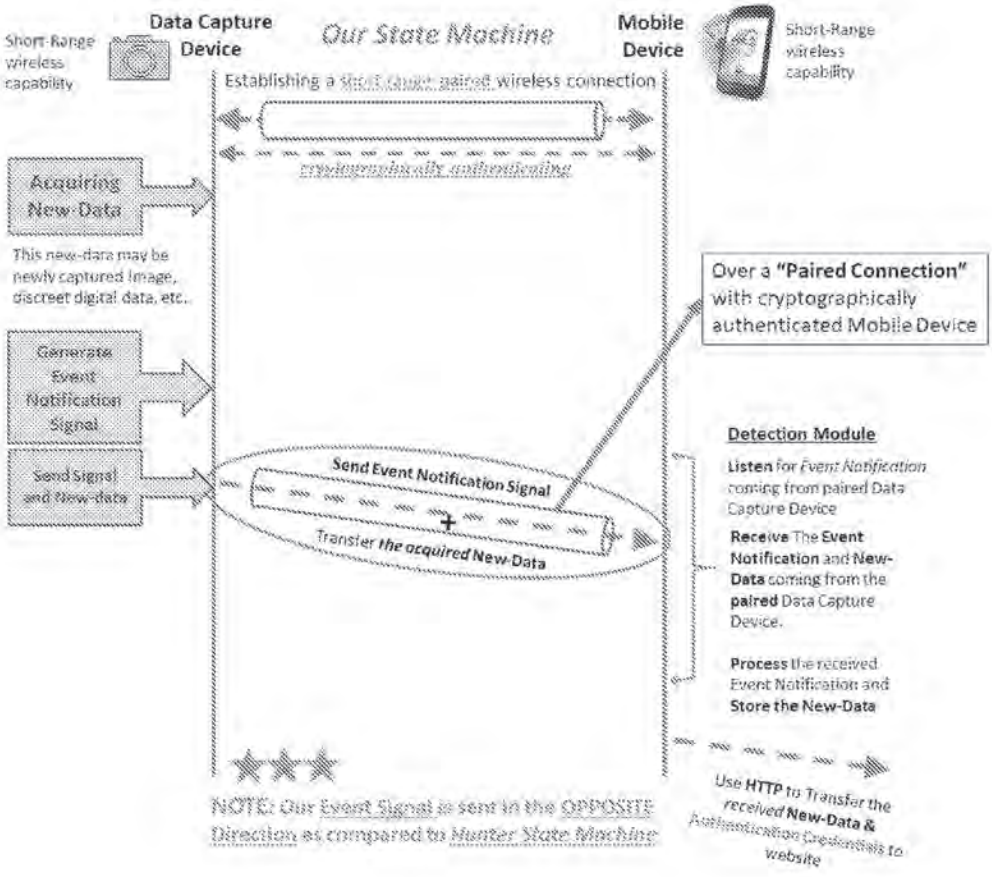
LifeScan, Inc. Ex. 1006
Page 236 of 353
IPR2025-00102

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, 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, wherein a 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, wherein the 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, 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 and the user authentication credential to a user data publishing website over a cellular data network, and wherein the mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data."

LifeScan, Inc. Ex. 1006
Page 237 of 353
IPR2025-00102

Summary

Applicant's state machine



LifeScan, Inc. Ex. 1006
Page 238 of 353
IPR2025-00102

Comparison Table

	Claim Feature	Hunter	Pietruszka	Applicant Cellspin
1	Pairing for new-data transfer.	NO mention of pairing. Pairing is NOT established. Teaching away from establishing permanent connection.	NO Invention is about selecting or preventing, and controlling pairing between devices. NOT for new data transfer	YES Pairing is established to transfer the acquired new data.
2	Cryptographically authenticate the identity of Mobile Device	NO	YES Only if wireless communication device is unlocked for pairing.	YES The Mobile device is cryptographically authenticated by the data capture device NOT based on pre-selection of activation or deactivation of pairing.
3	Sending new data capture Event Notification Signal	NO Trigger Event Signal is sent from the mobile device to the camera device, which is opposite to applicant's invention.	NO There is NO data capture Event signal sent to the cellular phone. There is NO data capture device.	YES Event Notification signal is sent from data capture device to cellular phone after acquiring new-data.
4	Send data to the mobile device over a pre-established paired connection	NO	NO There is no data to transfer.	YES
4	HTTP based transfer	NO HTTP is NOT used	NO There is No data to transfer.	YES HTTP is used as a data transport protocol
5	Is Timing of Data Acquisition after Pairing devices	NO	NO	YES After pairing is established
6	Data transfer between two devices happens over what type of wireless link?	NON-Paired wireless connection	NO data There is no new- data to transfer	Data over Paired wireless connection

In view of the above arguments, state machines and illustrative drawings, applicant submits that amended claim 1 is non-obvious over Hunter, in view of Pietruszka. Claims 4, 8 and 12 are analogous to claim 1, and include all the limitations of amended claim 1. Therefore, claims 4, 8 and 12 are also non-obvious over Hunter, in view of Pietruszka. Claims 2-3 are dependent on amended claim 1; claims 5-7 are dependent on amended claim 4; claim 9 is dependent on amended claim 8; claims 13-14 are dependent on amended claim 12. Applicant therefore submits that dependent claims 2-3, 5-7, 9 and 13-14 are also non-obvious over Hunter, in view of Pietruszka.

LifeScan, Inc. Ex. 1006
Page 239 of 353
IPR2025-00102

Applicant therefore respectfully requests that the rejection of claims 1-9 and 12-14 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

Claims 10-11 are cancelled. Therefore, the rejection of claims 10-11 is moot.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case. In the interest of compact prosecution, if the prosecution of the application can be advanced, applicant requests Examiner Nooristany to call the undersigned with the proposed amendment.

Respectfully submitted,

Date: January 20, 2021

/a tankha/
Ashok Tankha
Attorney For Applicant
Reg. No. 33,802

Correspondence Address
Lipton Weinberger & Husick
36 Greenleigh Drive
Sewell, NJ 08080
Phone: 856-266-5145
Email: ash@ipprocurement.com

LifeScan, Inc. Ex. 1006
Page 240 of 353
IPR2025-00102

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/532,507	08/06/2019	Gurvinder Singh	CellSpin_04Con17_US	6207

64188 7590 10/26/2020
ASHOK TANKHA
36 GREENLEIGH DRIVE
SEWELL, NJ 08080

EXAMINER
NOORISTANY, SULAIMAN

ART UNIT	PAPER NUMBER
2415	

NOTIFICATION DATE	DELIVERY MODE
10/26/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ASH@IPPROCUREMENT.COM
docketing1@ipprocurement.com
docketing@ipprocurement.com

PTOL-90A (Rev. 04/07)

LifeScan, Inc. Ex. 1006
Page 241 of 353
IPR2025-00102

Office Action Summary	Application No. 16/532,507	Applicant(s) Singh et al.	
	Examiner SULAIMAN NOORISTANY	Art Unit 2415	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on 10/16/20.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☑ This action is **FINAL.** 2b) ☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-14 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-14 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date 10/17/20, 10/20/20.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

aNotice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. More specifically, the applicant fails to sufficiently point out or describe

cellular phone remains paired after storing the created new-data;

a user authentication credential to a user data publishing website over the cellular data network"

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.

The specification of this application under examination does not contain subject matter to implement limitations, as cited in the following claims.

Also, it is not apparent how "***remains paired***" "***a user authentication credential to a user data publishing website over the cellular data network***" *as* recited in claim 1,4, is determined.

LifeScan, Inc. Ex. 1006
Page 243 of 353
IPR2025-00102

It is not apparent how "***wherein the user authentication credential is for a user of the user data publishing website***" *as* recited in claim 6, is determined

It is not apparent how "***authentication credentials use HTTP to send global positioning system information to the user data publishing website over the cellular data network***" *as* recited in claim 7, is determined.

Examiner has reviewed the specification of this application under examination (and OCR whole document) and could not find support for the additional limitations as claimed.

Specification Objection

The disclosure is objected to because of the following informalities: Examiner has reviewed the specification of this application under examination and could not find support for the additional limitations as claimed *"**remains paired***", "***a user authentication credential to a user data publishing website over the cellular data network***" "***use HTTP to send global positioning system information to the user data publishing website over the cellular data network***". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 1-14 are rejected under 112, second paragraph as being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention

LifeScan, Inc. Ex. 1006
Page 244 of 353
IPR2025-00102

In claim **4**, the terms *"**remains paired**", "**a user authentication credential to a user data publishing website over the cellular data network**"* are not clear what these are in reference to. Also, the description of the present application fails to provide a clear and complete description on the invention as well as the above terms. However, the claims will be given a broad reasonable interpretation for the purposes of examination as best understood.

In claim **6**, the terms *"**wherein the user authentication credential is for a user of the user data publishing website**"* are not clear what these are in reference to. Also, the description of the present application fails to provide a clear and complete description on the invention as well as the above terms. However, the claims will be given a broad reasonable interpretation for the purposes of examination as best understood.

In claim **7**, the terms *"**use HTTP to send global positioning system information to the user data publishing website over the cellular data network**"* are not clear what these are in reference to. Also, the description of the present application fails to provide a clear and complete description on the invention as well as the above terms. However, the claims will be given a broad reasonable interpretation for the purposes of examination as best understood.

Claims 1-3, 5-14 are rejected for similar reasons as stated for claim 4.

LifeScan, Inc. Ex. 1006
Page 245 of 353
IPR2025-00102

Claim Rejections - 35 USC § 103

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1-14 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778.

4. A system, comprising:

a short-range wireless enabled data capture device **(Hunter fig. 1, unit 10)**, comprising:

a first memory device **(Hunter: a camera with an image memory and a first wireless communication interface [0010] fig. 1, unit 10)**;

a first processor coupled to the first memory device **(Hunter: a camera with an image memory and a first wireless communication interface [0010] fig. 1, unit 10)**;

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 **(Hunter: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10**

LifeScan, Inc. Ex. 1006
Page 246 of 353
IPR2025-00102

to establish a data link between the two units. Alternatively, the camera 10 may periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10 [0017-0027, 0036-0037]).

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;

a data capture circuitry **(Hunter: fig. 1 unit 10)**;

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 **(Hunter: [0017-0027, 0036-0037] After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038])**;

said first processor further configured to store the new-data in the first memory device **(Hunter: After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038])**, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the created new-data

LifeScan, Inc. Ex. 1006
Page 247 of 353
IPR2025-00102

(Hunter: [0017-0027, 0036-0038] The wireless link may be pre-existing, or may be set up only on the initiation of the call [0039-0040]); and

said first processor further configured to send an event notification **(Hunter: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween [0013])** and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically **(Hunter: transferring images between the camera and the communications device over the wireless link [0013])**, 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 **(Hunter: [0013])**,

said short-range wireless enabled cellular phone **(Hunter: fig. 1 unit 20)**, comprising:

a second memory device **(Hunter: fig. 1 unit 20)**;

a second processor coupled to the second memory device **(Hunter: fig. 1 unit 20)**;

a cellular network communication device configured to connect to the internet via the cellular data network **(Hunter: fig. 1 unit 20)**;

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 **(Hunter: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10 to establish a data link between the two units. Alternatively, the camera 10 may periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to**

LifeScan, Inc. Ex. 1006
Page 248 of 353
IPR2025-00102

establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10 [0017-0027, 0036-0037]);

a 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 an event notification sent by the short-range wireless enabled data capture device, wherein a mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the event notification (**Hunter: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween [0013]**);

receive the new-data from the short-range wireless enabled data capture device (**Hunter: an image storage buffer 24 for storing image data received from the camera 10 [0035]**);

store the received new-data in the second memory device (**Hunter: an image storage buffer 24 for storing image data received from the camera 10 [0035]**), wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the received new-data (**Hunter: The wireless link may be pre-existing, or may be set up only on the initiation of the call [0017-0027, 0036-0037, 0039-0040]**); and

use HTTP to upload the received new-data and a user authentication credential to a user data publishing website over the cellular data network (**Hunter: transferring said images from the communications device on to a data network through a data network interface [0013, 0035, 0041]**).

LifeScan, Inc. Ex. 1006
Page 249 of 353
IPR2025-00102

Hunter merely discloses the term *cryptographically* authenticating

Pietruszka further teaches cryptographically authenticating (**Pietruszka: [0037]**) in order to communicate only with a trusted device can cryptographically authenticate the identity of the other device.

Thus, it would have been obvious to one skill in the art to include the above recited limitation into Hunter's in order to communicate only with a trusted device can cryptographically authenticate the identity of the other device [0037], as taught by Pietruszka.

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 **(Hunter: [0037])**

6. The system of claim 4, wherein mobile client application for the short-range wireless enabled cellular phone comprises executable instructions that, when executed by the second processor controls the second processor to:

store the user authentication credential in the second memory device, wherein the user authentication credential is for a user of the user data publishing website; and

provide a touch based graphical user interface for the received new-data **(Hunter: [0025], Pietruszka [0099])**

7. The system of claim 4, wherein data the mobile client application for the short-range wireless enabled cellular phone comprises executable instructions that, when executed by the

LifeScan, Inc. Ex. 1006
Page 250 of 353
IPR2025-00102

second processor controls the second processor to: use HTTP to send global positioning system information to the user data publishing website over the cellular data network **(Hunter: [0031])**

Regarding claims 1-3, 8-14 the independent claim and each dependent claim are related to the same limitation set for hereinabove in claims 4-7, where the difference used is a "capture device" & "mobile device" and the wordings of the claims were interchanged within the claim itself or some of the claims were presented as a combination of two or more previously presented limitations. This change does not affect the limitation of the above treated claims. Adding these phrases to the claims and interchanging the wording did not introduce new limitations to these claims. Therefore these claims were rejected for similar reasons as stated above

Response to Arguments

Applicant's arguments filed on 10/16/20 have been fully considered but they are not persuasive.

Applicant Argument:

Regarding first paragraph of 35 U.S.C. 112 rejection, Applicant is suggesting for support to some page Nos. 5, 7, 9 and Figure 2 and Figure 4 of US Non-provisional patent application serial number 11/901,802.

Response to Arguments:

With respect to the above argument, Examiner would like to draw attention that the US Non-provisional patent application serial number 11/901,802 has no relation to this current application. Thus, the Examiner maintains the rejection.

LifeScan, Inc. Ex. 1006
Page 251 of 353
IPR2025-00102

Applicant Argument:

Prior art failed to teach pairing short range wireless or away from permanent paired short-range wireless connection and cryptographic pairing between devices

Response to Arguments:

With respect to the above argument, Examiner would like to draw attention to that **it is the claims that define the claimed invention, and it is claims, not specifications that are anticipated or unpatentable. Constant v. Advanced Micro-Devices Inc., 7 USPQ2d 1064**.

In addition, the Examiner would like to draw attention to (fig. 1, [0017-0027, 0036-0037]) of **Hunter**, for example: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10 to establish a data link between the two units. Alternatively, the camera 10 may periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10.

The Examiner further would like to draw attention to ([0037]) of **Hunter**, for example: a device that wishes to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt data exchanged over a wireless medium as an added security. The encryption can however be turned off and passkeys can be stored on the device's file system rather than the Bluetooth component or chip itself. Since the Bluetooth address can be permanent, a pairing can be preserved even if the Bluetooth name is changed. Either device in a pairing relationship may delete the pairing between the devices. Devices may require pairing or may prompt the user before it allows a remote device to utilize

LifeScan, Inc. Ex. 1006
Page 252 of 353
IPR2025-00102

any or all or some of its services (*herein* **it's** considered same as *paired short-range wireless connection and cryptographic pairing between devices*).

Applicant Argument:

Prior art failed to teach receiving or making Phone call trigger even vs NO such Phone call trigger event.

Response to Arguments:

In addition, the Examiner would like to draw attention to (fig. 1, [0013]) of **Hunter**, for example: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween (*herein* **it's** considered same as *sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data*).

Applicant Argument:

Prior art failed to teach sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data.

LifeScan, Inc. Ex. 1006
Page 253 of 353
IPR2025-00102

Response to Arguments:

In addition, the Examiner would like to draw attention to (fig. 1, [0013]) of **Hunter**, for example: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween (*herein* **it's** considered same as *sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data*).

Applicant Argument:

Prior art failed to teach use HTTP to transfer new-data and a user authentication credential to website

Response to Arguments:

In addition, the Examiner would like to draw attention to (fig. 1, [0009, 0031, 0041]) of **Hunter**, for example: it is known for mobile telephones to support data instead of or as well as voice calls, in which case the present invention can be taken to relate also to the establishment of a data link or the initiation of data transmission as a result of use of a telephone to access a data service, e.g. an internet page such as a photo website or a photo printing service (*herein* **it's** considered same as *use HTTP to transfer new-data and a user authentication credential to website*).

LifeScan, Inc. Ex. 1006
Page 254 of 353
IPR2025-00102

Thus, for the above reason, the prior art meet the claim limitation.

The examiner stresses that the claims are too broad and require detail or specialization of the steps as recited in the claims. Alone and as claimed, the limitations are too open.

Examiner has cited particular portions of the references as applied to each claim limitation for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Regarding all other arguments presented by applicant, the arguments are substantially the same as those which have already been addressed above and in the interest of brevity; the Examiner directs the applicant to those responses above.

Remark:

In addition, an interview could expedite the prosecution.

Conclusion

Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory

LifeScan, Inc. Ex. 1006
Page 255 of 353
IPR2025-00102

period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sulaiman Nooristany whose telephone number is 571-270-1929. The examiner can normally be reached on Monday thru Friday: 8:30am to 5:00pm (EST). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Rutkowski can be reached on 571-270-1215. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/SULAIMAN NOORISTANY/

Primary Examiner, Art Unit 2415

LifeScan, Inc. Ex. 1006
Page 256 of 353
IPR2025-00102

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re. application of:
Gurvinder Singh
Application No.: 16/532,507 Examiner: Nooristany, Sulaiman
Filed: 08/06/2019 Art Unit: 2415
Applicant: Cellspinsoft Inc. Atty. Docket no.: CellSpin_04Con17_US
Title: Automatic Multimedia Upload
For Publishing Data And Multimedia Content

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Response to Non-Final Office Action

Examiner Nooristany:

In response to the non-final office action mailed July 17, 2020, please amend the above-referenced application as follows:

Amendments to the Claims are listed on page 2 of this response.

Remarks begin on page 13 of this response.

LifeScan, Inc. Ex. 1006
Page 257 of 353
IPR2025-00102

Amendments to the claims

Claim 1 (currently amended): A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the created new-data;

said processor further configured to send an event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled

LifeScan, Inc. Ex. 1006
Page 258 of 353
IPR2025-00102

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, 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, wherein a 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, 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 and ~~user publication information~~ a user authentication credential to a user data publishing website over a cellular data network~~, wherein the user publication information comprises user preferences, and wherein the user preferences comprise authentication credentials and global positioning system information~~.

Claim 2 (previously presented): 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.

Claim 3 (currently amended): 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~~ mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone stores the user authentication credential in a non-volatile memory device of the cryptographically authenticated short-range wireless enabled cellular phone, wherein the user authentication credential sent by the 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

LifeScan, Inc. Ex. 1006
Page 259 of 353
IPR2025-00102

user data publishing website, and wherein the mobile client application provides a touch based GUI for the received new-data.

Claim 4 (currently amended): A system, comprising:

a short-range wireless enabled data capture device, comprising:

a first memory device;

a first processor coupled to the first memory device;

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;

a data capture circuitry;

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;

said first processor further configured to store the new-data in the first memory device, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device

and the short-range wireless enabled cellular phone remains paired after storing the created new-data; and

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;

said short-range wireless enabled cellular phone, comprising:

a second memory device;

a second processor coupled to the second memory device;

a cellular network communication device configured to connect to the internet via [[the]] a cellular data network;

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;

a 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 [[an]] the event notification sent by the short-range wireless enabled data capture device, wherein [[a]] the mobile client application for the cryptographically authenticated short-

LifeScan, Inc. Ex. 1006
Page 261 of 353
IPR2025-00102

range wireless enabled cellular phone is configured to process the event notification;

receive the new-data from the short-range wireless enabled data capture device;

store the received new-data in the second memory device, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the received new-data; and

use HTTP to upload the received new-data and a user ~~publication information~~ authentication credential to a user data publishing website over the cellular data network~~, wherein the user publication information comprises user preferences, and wherein the user preferences comprise authentication credentials and global positioning system information~~.

Claim 5 (previously presented): 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.

Claim 6 (currently amended): 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~~ mobile client application for the short-range wireless enabled cellular phone comprises executable instructions that, when executed by the second processor controls the second processor to:

store the user authentication credential in the second memory device, wherein the user authentication credential is for a user of the user data publishing website; and

provide a touch based graphical user interface for the received new-data.

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

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

Claim 8 (currently amended): A short-range wireless enabled cellular phone, comprising:

a memory device;

a processor coupled to the memory device;

a cellular network communication device configured to connect to internet via a cellular data network;

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;

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:

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 cryptographically authenticated 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;

receive the event notification and the new-data from the short-range wireless enabled data capture device;

process the event notification and store the received new-data in the ~~second~~ memory device, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the received new-data; and

use HTTP to upload the received new-data and a user ~~publication information~~ authentication credential to a user data publishing ~~website~~ web service over the cellular data network~~, wherein the user publication information comprises user preferences, and wherein the user preferences comprise authentication credentials and global positioning system information~~.

Claim 9 (previously presented): The short-range wireless enabled cellular phone of claim 8, 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.

Claim 10 (currently amended): The short-range wireless enabled cellular phone of claim 8, 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~~ the mobile client application for the short-range wireless enabled cellular phone comprises executable instructions that, when executed by the processor controls the processor to:

store the user authentication credential in the memory device, and

provide a touch based graphical user interface for the received new-data.

Claim 11 (currently amended): The short-range wireless enabled cellular phone of claim 8, 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~~ the mobile client application for the short-range wireless enabled cellular phone comprises executable instructions that, when executed by the processor controls the processor to:

use HTTP to send global positioning system information to the user data publishing web service over the cellular data network.

Claim 12 (currently amended): A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

LifeScan, Inc. Ex. 1006
Page 265 of 353
IPR2025-00102

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device of the short-range wireless enabled data capture device, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the created new-data;

said processor further configured to listen to a polling request from a mobile client application on the cryptographically authenticated short-range wireless enabled cellular phone, over the established paired short-range wireless connection, wherein the polling request is for the new-data, wherein the mobile client application on the cryptographically authenticated 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 authenticated short-range wireless enabled cellular phone, wherein detecting the new-data for transfer comprises:

LifeScan, Inc. Ex. 1006
Page 266 of 353
IPR2025-00102

polling the short-range wireless enabled data capture device by the short-range wireless enabled cellular phone, using the mobile client application on the cryptographically authenticated short-range wireless enabled cellular phone, over the established paired short-range wireless connection;

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 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 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 mobile client application on the short-range wireless enabled cellular phone is further configured to use HTTP to upload the received new-data and a user ~~publication information~~ authentication credential to a user data publishing website over a cellular data network~~, wherein the user publication information comprises user preferences, and wherein the user preferences comprise authentication credentials and global positioning system information~~.

Claim 13 (previously presented): The short-range wireless enabled data capture device of claim 12, 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.

Claim 14 (currently amended): The short-range wireless enabled data capture device of claim 12, 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~~ mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone stores the user authentication credential in a non-volatile memory device of the

LifeScan, Inc. Ex. 1006
Page 267 of 353
IPR2025-00102

cryptographically authenticated short-range wireless enabled cellular phone, and wherein the mobile client application provides a touch based GUI for the received new-data.

LifeScan, Inc. Ex. 1006
Page 268 of 353
IPR2025-00102

Remarks

The pending claims

Claims 1-14 are currently pending. Reconsideration and allowance of the pending claims is respectfully requested.

Summary of the Office Action

Claim Rejections 35 U.S.C. 112

Claims 1-14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. More specifically, the applicant fails to sufficiently point out or describe: "*cellular phone remains paired after storing the created new-data*"; and "*wherein the user preferences comprise authentication credentials and global positioning system information.*"

Specification Objection

The disclosure is objected to because of the following informalities: Examiner has reviewed the specification of this application under examination and could not find support for the additional limitations as claimed "*remains paired*" & "*authentication credentials and global positioning system information*". Appropriate correction is required.

Claim Rejections - 35 USC § 112

LifeScan, Inc. Ex. 1006
Page 269 of 353
IPR2025-00102

Claims 1-14 are rejected under 112, second paragraph as being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention. In claim 4, the terms "*remains paired*" & "*authentication credentials*" and "*global positioning system information*" are not clear what these are in reference to. Also, the description of the present application fails to provide a clear and complete description on the invention as well as the above terms. However, the claims will be given a broad reasonable interpretation for the purposes of examination as best understood. Claims 1-3, 5-14 are rejected for similar reasons as stated for claim 4.

Claim Rejections 35 U.S.C. 103

Claim 1-14 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778.

Amendments to the claims

Claims 1, 3-4, 6-8 and 10-12 and 14 are currently amended; claims 2, 5, 9 and 13 remain as previously presented. Applicant respectfully submits that the amendments to the claims do not add any new subject matter.

The office action states: "**Claims 1-14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. More specifically, the applicant fails to sufficiently point out or describe: "*cellular phone remains paired after storing the created new-data*"; and "*wherein the user preferences comprise authentication credentials and global positioning system information*.**"

Applicant disagrees with the above rejection and presents the following arguments:

Point No. 2 of "*CROSS REFERENCE TO RELATED APPLICATIONS*" in the originally filed application states as follows: "*The following patent application is* ***incorporated herein in its entirety****: US Non-provisional patent application serial number 11/901,802, titled "Online Publishing of Multimedia Content", filed on September 19, 2007 in the United States Patent and Trademark Office.*" USPTO Publication No. 2008/0103906 A1 is the published application of US Non-provisional patent application serial number 11/901,802. US Non-provisional patent application serial number 11/901,802 is attached to this response as Exhibit A and USPTO Publication No. 2008/0103906 A1 is attached to this response as Exhibit B; see also link: https://patentimages.storage.googleapis.com/1f/06/a0/32f9a69fbef2a6/US20080103906A1.pdf.

Page Nos. 5, 7, 9 and Figure 2 and Figure 4 of US Non-provisional patent application serial number 11/901,802 (Exhibit A) reproduced below disclose that the client application is *having and sending* "*authentication credentials*" and "*global positioning system geographical codes*" to the publishing website. The corresponding sections in Exhibit B are:

Extract from Page 9 of Exhibit A = Paragraph [0028] in Exhibit B.

Extract from Page 5 of Exhibit A = Paragraph [0018] in Exhibit B.

Extract from Page 7 of Exhibit A = Paragraph [0023] in Exhibit B.

Page 9

Before the recording begins, the user **201** may change the default publication location, and select the publication virtual spaces **205** for the user created multimedia content on the mobile device. The user **201** may also change the quality of the media before recording the message. For example, if compression is available, the user **201** may change the compression rate, and also change both the transfer speed and message quality. 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, 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. These user preferences are transferred to the publishing service **204**.

15

LifeScan, Inc. Ex. 1006
Page 271 of 353
IPR2025-00102

The method disclosed herein further provides **103** the publishing service **204** comprising a front end service **204b** and a back end service **204c**. The client application **202** interacts with the publishing service **204** to determine the preferred websites or publication virtual spaces **205** of the user **201** for publishing the user created multimedia content. The user **201** may select one or more publication virtual spaces **205** using the client application **202**, as a preferred destination for publishing the user created multimedia content. The client application **202** communicates the user publishing information including the user preferences of the publication virtual spaces **205** to the front end service **204b**. In one embodiment, the publication virtual spaces **205** may be selected on the website of the publishing service **204**. The method disclosed herein provides a protocol for synchronizing **104** user publishing information between the client application **202** and the publishing service **204**. The user publishing information includes user preferences of the publication virtual spaces **205**. The user created multimedia content is received by the front end service **204b** of the publishing service **204** from the client application **202** and then transferred **105** to the back end service **204c** of the publishing service **204**.

Page 5

Furthermore, "Authentication credentials" or "credentials for user authentication" or just "credentials" are mentioned **5** times in the US Non-provisional patent application serial number 11/901,802 on pages 7, 9, 12, 13 and in FIGURE 4.

LifeScan, Inc. Ex. 1006
Page 272 of 353
IPR2025-00102

The multimedia object is then transferred **107** from the back end service **204c** to the front end service **204b**. The multimedia object is published **108** by the front end service **204b** according to the user preferences on one or more publication virtual spaces **205** via the network **203**. The user preferences may comprise authentication credentials, transaction identification, a 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 a compression rate of the multimedia content. The user **201** stores these preferences during registration with the publishing service **204**. The publishing service **204** may also collect viewing information each time the multimedia object is viewed on the publication virtual spaces **205**. The viewing information is used to generate advertising statistics. The multimedia object may be published by a single input action of the user **201**. 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, a voice command, or a turn of a scroll wheel on the mobile device.

LifeScan, Inc. Ex. 1006
Page 273 of 353
IPR2025-00102

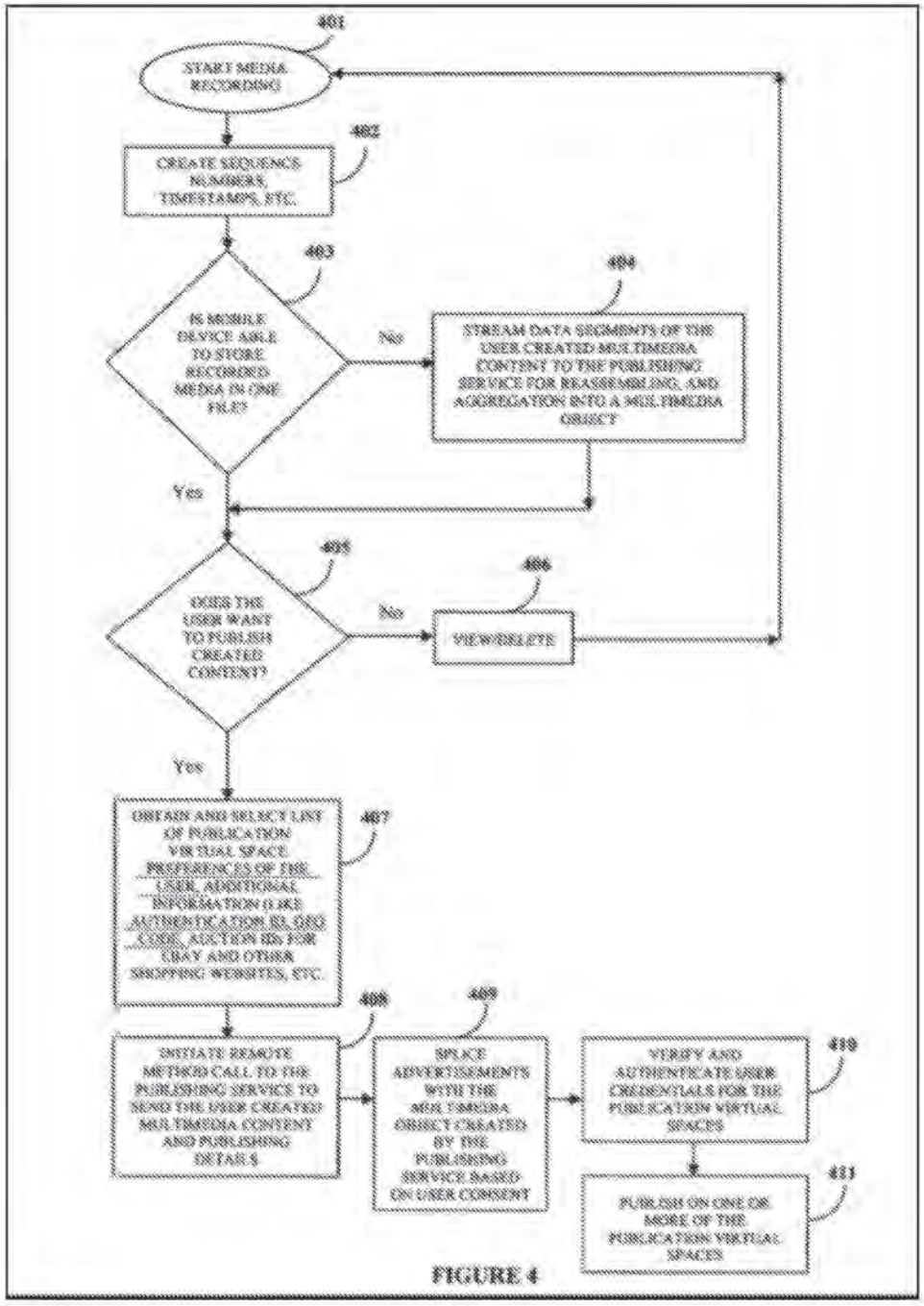


FIGURE 4

Furthermore, "global positioning system geographical codes" is mentioned **twice** in the U.S. No. 11/901,802 on **page 7 and page 9.**

18

LifeScan, Inc. Ex. 1006
Page 274 of 353
IPR2025-00102

Furthermore, "Authentication" as a module is present on the client application and the publishing service as shown in FIGURE 2 of U.S. No. 11/901,802 as highlighted below.

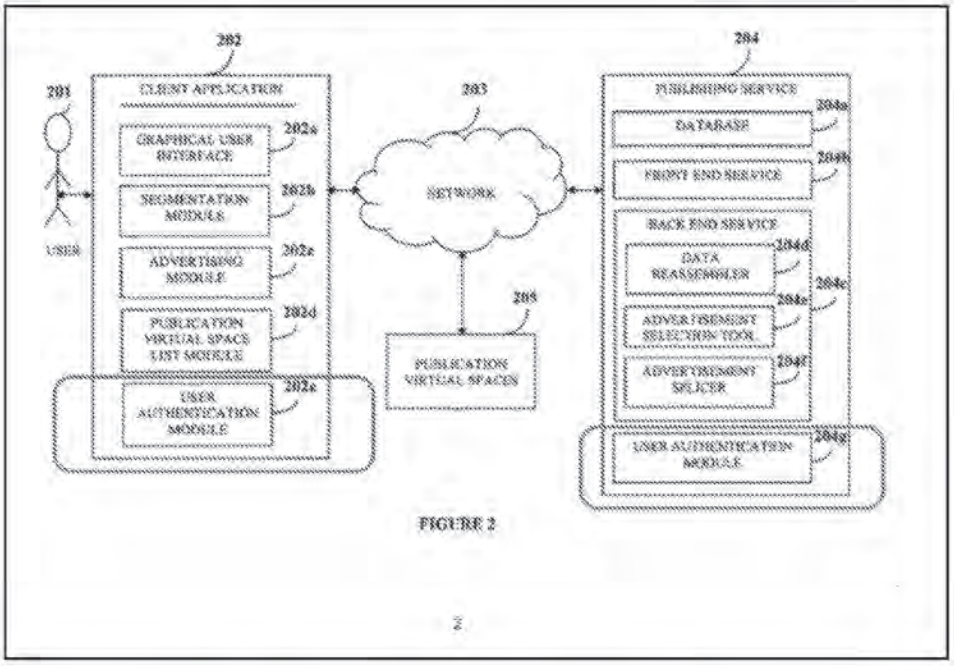


FIGURE 2

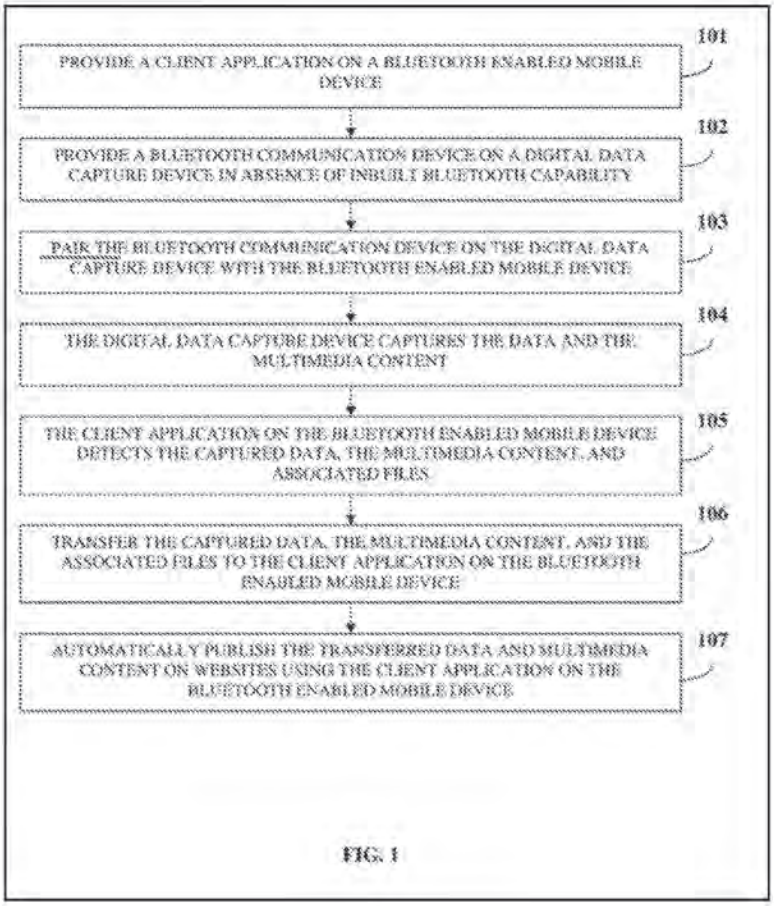
Furthermore, "Authentication" as a process step being performed in the state machine is explained in FIGURE 4 of U.S. No. 11/901,802 as highlighted above.

In response to the above rejection, applicant has amended claims 1, 4, 8 and 12, and submits that the amended claims do not contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention.

Furthermore, with respect to *"remains paired"* **nowhere in the specification applicant has used the word "*disconnect*" or "*unpair*" the established paired**

LifeScan, Inc. Ex. 1006
Page 275 of 353
IPR2025-00102

connection. The paired connection once paired in the state machine is intended to remain paired. **There is NO mention of unpairing in the state machine of Fig 1. The "*remains paired*" is inherent in the specification and the state machine of Fig 1 because there is no unpairing.**



Short-range Pairing and **Paired wireless connection** are terms in the art of wireless technology and has been known and was used in the wireless industry for almost 10 years before the Cellspin patent's priority date of December 2007. Bluetooth wireless standard organization was the first to introduce the term "Bluetooth" at the Blackberry technology consortium in 1998; see Exhibit C, also available at the link: https://web.archive.org/web/20180525083558/https://www.bluetooth.com/about-us/our-

history. Furthermore, in 1999, the detailed Bluetooth 1.0 specification with pairing was released; see Exhibit D attached to this response; also available at the link: http://grouper.ieee.org/groups/802/15/Bluetooth/profile_10_b.pdf.

The concept of a short-range paired connection, as established by the **Bluetooth** Special Interest Group (**Bluetooth SIG**), became known and adopted by certain other industry organizations creating wireless technology for device connections, such as WiFi Alliance and Zigbee Forum. In the context of wireless connections, the term "pairing" was adopted by the wireless industry almost 10 years before the Cellspin patent's priority date of December 2007. Drawing from wireless industry's understanding of the term "*paired wireless connection*" / pairing, the **broadest reasonable interpretation** (BRI) of "*paired wireless connection*" as understood by POSITA in Dec 2007, i.e. 10 years after the term was introduced in the wireless lexicon is:

> "bidirectional communications link between devices which provides for encrypted data exchange between the devices, and the communication link can be disconnected and reconnected without having to repeat pairing or authentication."

As explained above, POSITA understands that unless there is a specific mention of "unpair" "unpairing" the devices that are "paired" in a given state machine, those devices "remain paired" over an extended period of time. Unless and until there is an explicit call for *unpairing/unpair* the devices in that particular state machine or there is an action to remove/delete the pairing table from the device. None of applicant's state machine or the specification call for *unpairing/unpair or* remove/delete the pairing table.

Because short-range "pairing" is a well-understood term in the art, the applicant followed Federal Court's direction that the **"patent need not teach, and preferably omits, what is well known in the art."** *See McRO, Inc. v. Bandai Namco Games Am. Inc., 959 F.3d 1091, 1102 (Fed. Cir. 2020).* In conformance with this guidance, the applicant cited a version of "pairing" at least 50 times without explicitly defining it.

LifeScan, Inc. Ex. 1006
Page 277 of 353
IPR2025-00102

Additionally, while not explicitly defining "pairing," the applicant provided guidance to a POSITA that short-range "pairing" should conform to Bluetooth's conception of the term, which was later adopted when ZigBee and WiFi adopted pairing, making it the only definition applicable to short-range paired wireless connections whether or not a Bluetooth Connection.

Applicant therefore respectfully requests that the rejection of claim 1 under 35 U.S.C. 112, first paragraph be reconsidered and withdrawn.

Claims 4, 8 and 12 are analogous to claim 1. Applicant therefore respectfully requests that the rejection of claims 4, 8 and 12 under 35 U.S.C. 112, first paragraph be reconsidered and withdrawn.

Claims 2-3 are dependent on claim 1. Claims 5-7 are dependent on claim 4. Claims 9-11 are dependent on claim 8. Claims 13-14 are dependent on claim 12. Applicant therefore respectfully requests that the rejection of claims 2-3, 5-7, 9-11, and 13-14 under 35 U.S.C. 112, first paragraph be reconsidered and withdrawn.

The office action further states: "**The disclosure is objected to because of the following informalities: Examiner has reviewed the specification of this application under examination and could not find support for the additional limitations as claimed "*remains paired*" & *"authentication credentials and global positioning system information"*. Appropriate correction is required.**"

In response to the above objection, applicant submits the following arguments.

Point No. 2 of "*CROSS REFERENCE TO RELATED APPLICATIONS*" in the originally filed application states as follows: "*The following patent application is **incorporated herein in its entirety**: US Non-provisional patent application serial number 11/901,802, titled "Online Publishing of Multimedia Content", filed on September 19, 2007 in the United States Patent and Trademark Office.*" USPTO Publication No.

LifeScan, Inc. Ex. 1006
Page 278 of 353
IPR2025-00102

2008/0103906 A1 is the published application of US Non-provisional patent application serial number 11/901,802. US Non-provisional patent application serial number 11/901,802 is attached to this response as Exhibit A and USPTO Publication No. 2008/0103906 A1 is attached to this response as Exhibit B.

Page Nos. 5, 7, 9 and Figure 2 and Figure 4 of US Non-provisional patent application serial number 11/901,802 reproduced below disclose that the client application is *having and sending "authentication credentials"* and *"global positioning system geographical codes"* to the publishing website. The corresponding sections in Exhibit B are:

Extract from Page 9 of Exhibit A = Paragraph [0028] in Exhibit B.
Extract from Page 5 of Exhibit A = Paragraph [0018] in Exhibit B.
Extract from Page 7 of Exhibit A = Paragraph [0023] in Exhibit B.

Page 9

Before the recording begins, the user **201** may change the default publication location, and select the publication virtual spaces **205** for the user created multimedia content on the mobile device. The user **201** may also change the quality of the media before recording the message. For example, if compression is available, the user **201** may change the compression rate, and also change both the transfer speed and message quality. 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, 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. These user preferences are transferred to the publishing service **204**.

The method disclosed herein further provides **103** the publishing service **204** comprising a front end service **204b** and a back end service **204c**. The client application **202** interacts with the publishing service **204** to determine the preferred websites or publication virtual spaces **205** of the user **201** for publishing the user created multimedia content. The user **201** may select one or more publication virtual spaces **205** using the client application **202**, as a preferred destination for publishing the user created multimedia content. The client application **202** communicates the user publishing information including the user preferences of the publication virtual spaces **205** to the front end service **204b**. In one embodiment, the publication virtual spaces **205** may be selected on the website of the publishing service **204**. The method disclosed herein provides a protocol for synchronizing **104** user publishing information between the client application **202** and the publishing service **204**. The user publishing information includes user preferences of the publication virtual spaces **205**. The user created multimedia content is received by the front end service **204b** of the publishing service **204** from the client application **202** and then transferred **105** to the back end service **204c** of the publishing service **204**.

Page 5

Furthermore, "Authentication credentials" or "credentials for user authentication" or just "credentials" are mentioned **5** times in the US Non-provisional patent application serial number 11/901,802 on pages 7, 9, 12, 13 and in FIGURE 4.

The multimedia object is then transferred **107** from the back end service **204c** to the front end service **204b**. The multimedia object is published **108** by the front end service **204b** according to the user preferences on one or more publication virtual spaces **205** via the network **203**. The user preferences may comprise authentication credentials, transaction identification, a 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 a compression rate of the multimedia content. The user **201** stores these preferences during registration with the publishing service **204**. The publishing service **204** may also collect viewing information each time the multimedia object is viewed on the publication virtual spaces **205**. The viewing information is used to generate advertising statistics. The multimedia object may be published by a single input action of the user **201**. 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, a voice command, or a turn of a scroll wheel on the mobile device.

LifeScan, Inc. Ex. 1006
Page 281 of 353
IPR2025-00102

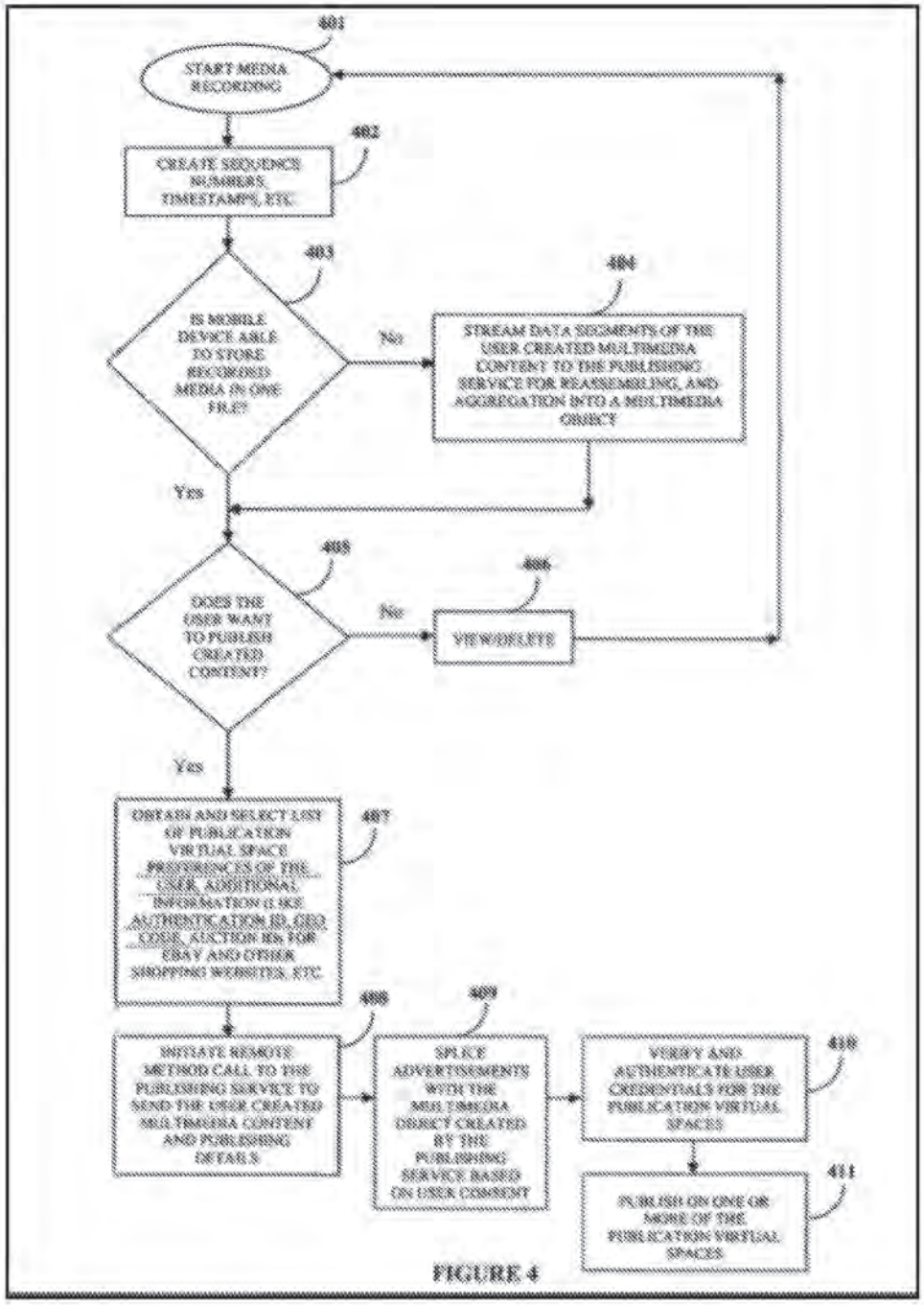


FIGURE 4

Furthermore, "global positioning system geographical codes" is mentioned **twice** in the U.S. No. 11/901,802 on page 7 and page 9.

Furthermore, "Authentication" as a module is present on the client application and the publishing service as shown in FIGURE 2 of U.S. No. 11/901,802 as highlighted below.

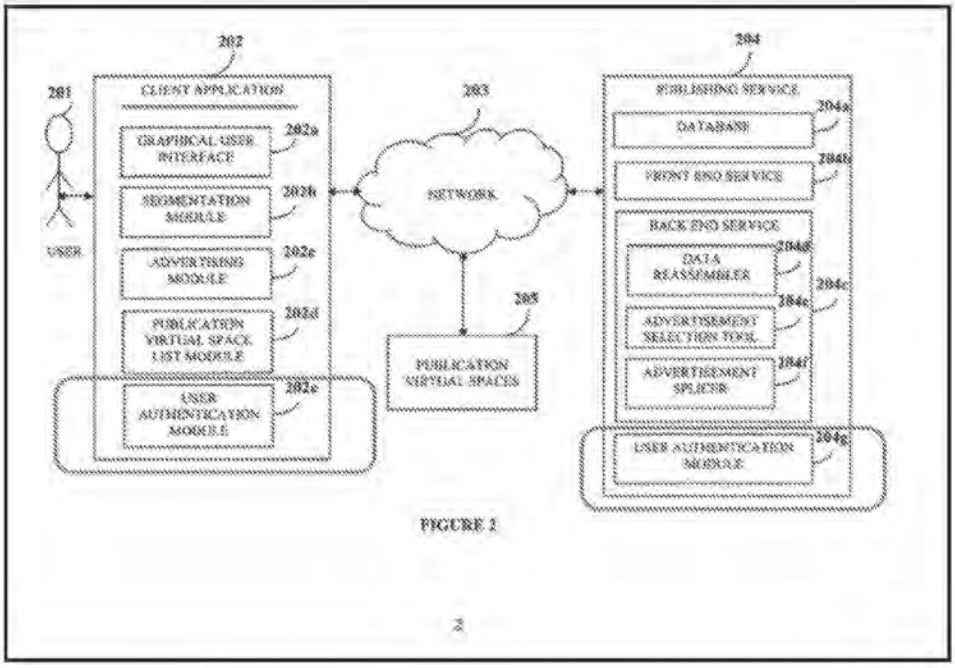


FIGURE 2

Furthermore, "Authentication" as a process step being performed in the state machine is explained in FIGURE 4 of U.S. No. 11/901,802 as highlighted above.

In response to the above rejection, applicant has amended claims 1, 4, 8 and 12, and submits that the amended claims do not contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention.

Furthermore, with respect to *"remains paired"* **nowhere in the specification applicant has used the word "*disconnect*" or "*unpair*" the established paired connection.** The paired connection once paired in the state machine is intended to remain paired. **There is NO mention of unpairing in the state machine of Fig 1. The "*remains paired*" is inherent in the specification and the state machine of Fig 1 because there is no unpairing.**

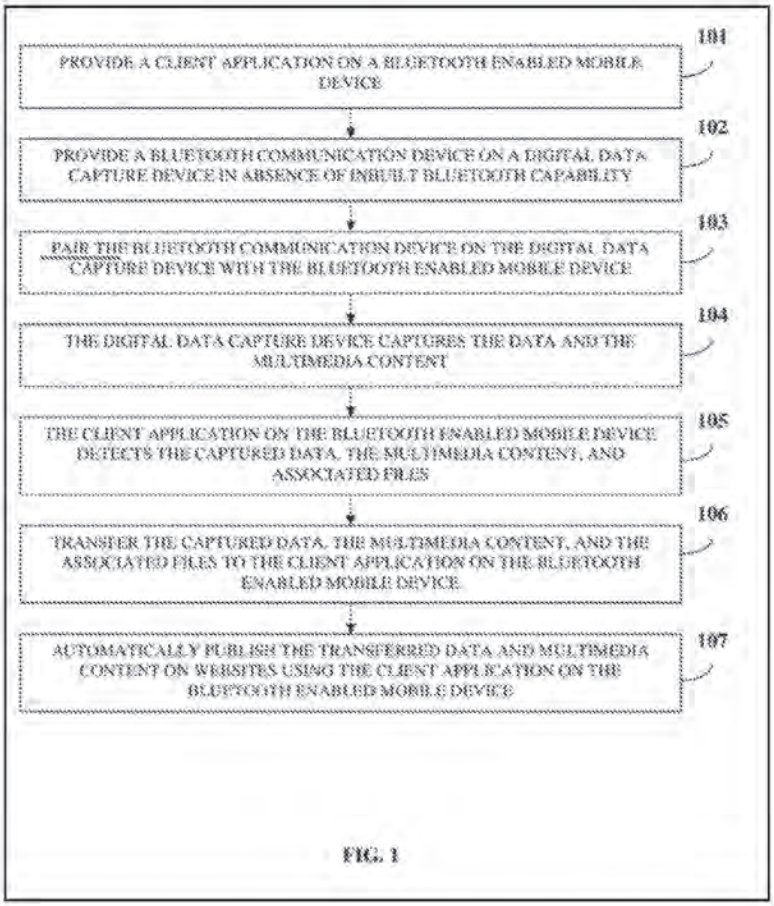


FIG. 1

Short-range Pairing and **Paired wireless connection** are terms in the art of wireless technology and has been known and was used in the wireless industry for almost 10 years before the Cellspin patent's priority date of December 2007. Bluetooth wireless standard organization was the first to introduce the term "Bluetooth" at the Blackberry

technology consortium in 1998; see Exhibit C, also available at the link: https://web.archive.org/web/20180525083558/https://www.bluetooth.com/about-us/our-history. Furthermore, in 1999, the detailed Bluetooth 1.0 specification with pairing was released; see Exhibit D attached to this response; also available at the link: http://grouper.ieee.org/groups/802/15/Bluetooth/profile_10_b.pdf.

The concept of a short-range paired connection, as established by the **Bluetooth** Special Interest Group (**Bluetooth SIG**), became known and adopted by certain other industry organizations creating wireless technology for device connections, such as WiFi Alliance and Zigbee Forum. In the context of wireless connections, the term "pairing" was adopted by the wireless industry almost 10 years before the Cellspin patent's priority date of December 2007. Drawing from wireless industry's understanding of the term "*paired wireless connection*" / pairing, the **broadest reasonable interpretation** (BRI) of "*paired wireless connection*" as understood by POSITA in Dec 2007, i.e. 10 years after the term was introduced in the wireless lexicon is:

> "bidirectional communications link between devices which provides for encrypted data exchange between the devices, and the communication link can be disconnected and reconnected without having to repeat pairing or authentication."

As explained above, POSITA understands that unless there is a specific mention of "unpair" "unpairing" the devices that are "paired" in a given state machine, those devices "remain paired" over an extended period of time. Unless and until there is an explicit call for *unpairing/unpair* the devices in that particular state machine or there is an action to remove/delete the pairing table from the device. None of applicant's state machine or the specification call for *unpairing/unpair or* remove/delete the pairing table.

Because short-range "pairing" is a well-understood term in the art, the applicant followed Federal Court's direction that the **"patent need not teach, and preferably omits, what is well known in the art."** *See McRO, Inc. v. Bandai Namco Games Am.*

LifeScan, Inc. Ex. 1006
Page 285 of 353
IPR2025-00102

Inc., 959 F.3d 1091, 1102 (Fed. Cir. 2020). In conformance with this guidance, the applicant cited a version of "pairing" at least 50 times without explicitly defining it. Additionally, while not explicitly defining "pairing," the applicant provided guidance to a POSITA that short-range "pairing" should conform to Bluetooth's conception of the term, which was later adopted when ZigBee and WiFi adopted pairing, making it the only definition applicable to short-range paired wireless connections whether or not a Bluetooth Connection.

Applicant therefore respectfully requests that the objection to the specification be reconsidered and withdrawn.

The office action further states: "**Claims 1-14 are rejected under 112, second paragraph as being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention. In claim 4, the terms "*remains paired*" & "*authentication credentials*" and "*global positioning system information*" are not clear what these are in reference to. Also, the description of the present application fails to provide a clear and complete description on the invention as well as the above terms. However, the claims will be given a broad reasonable interpretation for the purposes of examination as best understood. Claims 1-3, 5-14 are rejected for similar reasons as stated for claim 4.**"

Applicant disagrees with the above rejection and presents the following arguments:

Point No. 2 of "*CROSS REFERENCE TO RELATED APPLICATIONS*" in the originally filed application states as follows: "*The following patent application is* ***incorporated herein in its entirety****: US Non-provisional patent application serial number 11/901,802, titled "Online Publishing of Multimedia Content", filed on September 19, 2007 in the United States Patent and Trademark Office.*" USPTO Publication No. 2008/0103906 A1 is the published application of US Non-provisional patent application serial number 11/901,802. US Non-provisional patent application serial number

LifeScan, Inc. Ex. 1006
Page 286 of 353
IPR2025-00102

11/901,802 is attached to this response as Exhibit A and USPTO Publication No. 2008/0103906 A1 is attached to this response as Exhibit B.

Page Nos. 5, 7, 9 and Figure 2 and Figure 4 of US Non-provisional patent application serial number 11/901,802 reproduced below disclose that the client application is *having and sending "authentication credentials"* and "*global positioning system geographical codes*" to the publishing website. The corresponding sections in Exhibit B are:

Extract from Page 9 of Exhibit A = Paragraph [0028] in Exhibit B.
Extract from Page 5 of Exhibit A = Paragraph [0018] in Exhibit B.
Extract from Page 7 of Exhibit A = Paragraph [0023] in Exhibit B.

Page 9

Before the recording begins, the user **201** may change the default publication location, and select the publication virtual spaces **205** for the user created multimedia content on the mobile device. The user **201** may also change the quality of the media before recording the message. For example, if compression is available, the user **201** may change the compression rate, and also change both the transfer speed and message quality. 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, 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. These user preferences are transferred to the publishing service **204**.

The method disclosed herein further provides **103** the publishing service **204** comprising a front end service **204b** and a back end service **204c**. The client application **202** interacts with the publishing service **204** to determine the preferred websites or publication virtual spaces **205** of the user **201** for publishing the user created multimedia content. The user **201** may select one or more publication virtual spaces **205** using the client application **202**, as a preferred destination for publishing the user created multimedia content. The client application **202** communicates the user publishing information including the user preferences of the publication virtual spaces **205** to the front end service **204b**. In one embodiment, the publication virtual spaces **205** may be selected on the website of the publishing service **204**. The method disclosed herein provides a protocol for synchronizing **104** user publishing information between the client application **202** and the publishing service **204**. The user publishing information includes user preferences of the publication virtual spaces **205**. The user created multimedia content is received by the front end service **204b** of the publishing service **204** from the client application **202** and then transferred **105** to the back end service **204c** of the publishing service **204**.

Page 5

Furthermore, "Authentication credentials" or "credentials for user authentication" or just "credentials" are mentioned **5** times in the US Non-provisional patent application serial number 11/901,802 on pages 7, 9, 12, 13 and in FIGURE 4.

LifeScan, Inc. Ex. 1006
Page 288 of 353
IPR2025-00102

The multimedia object is then transferred **107** from the back end service **204c** to the front end service **204b**. The multimedia object is published **108** by the front end service **204b** according to the user preferences on one or more publication virtual spaces **205** via the network **203**. The user preferences may comprise authentication credentials, transaction identification, a 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 a compression rate of the multimedia content. The user **201** stores these preferences during registration with the publishing service **204**. The publishing service **204** may also collect viewing information each time the multimedia object is viewed on the publication virtual spaces **205**. The viewing information is used to generate advertising statistics. The multimedia object may be published by a single input action of the user **201**. 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, a voice command, or a turn of a scroll wheel on the mobile device.

LifeScan, Inc. Ex. 1006
Page 289 of 353
IPR2025-00102

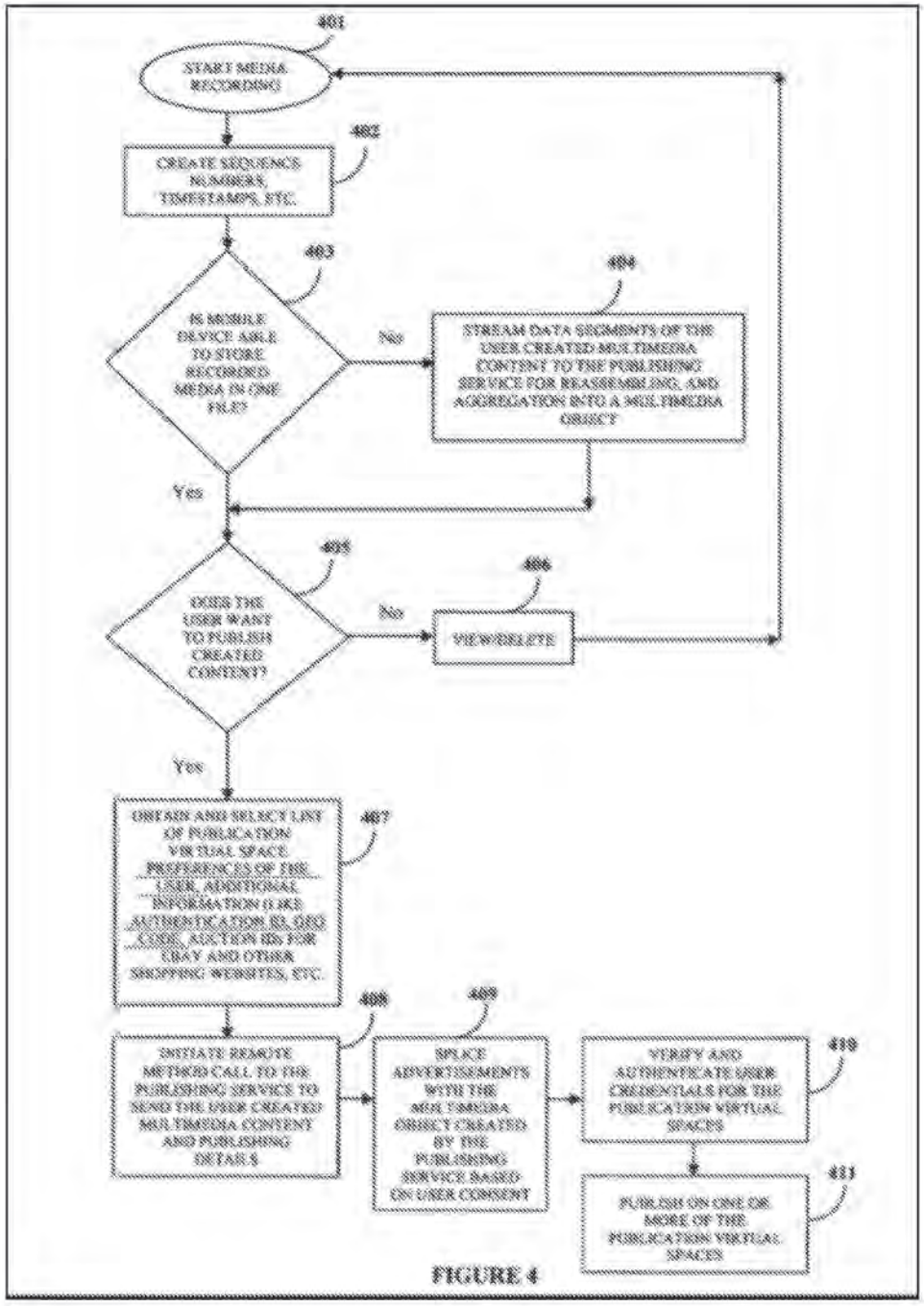


FIGURE 4

Furthermore, "global positioning system geographical codes" is mentioned **twice** in the U.S. No. 11/901,802 on page 7 and page 9.

Furthermore, "Authentication" as a module is present on the client application and the publishing service as shown in FIGURE 2 of U.S. No. 11/901,802 as highlighted below.

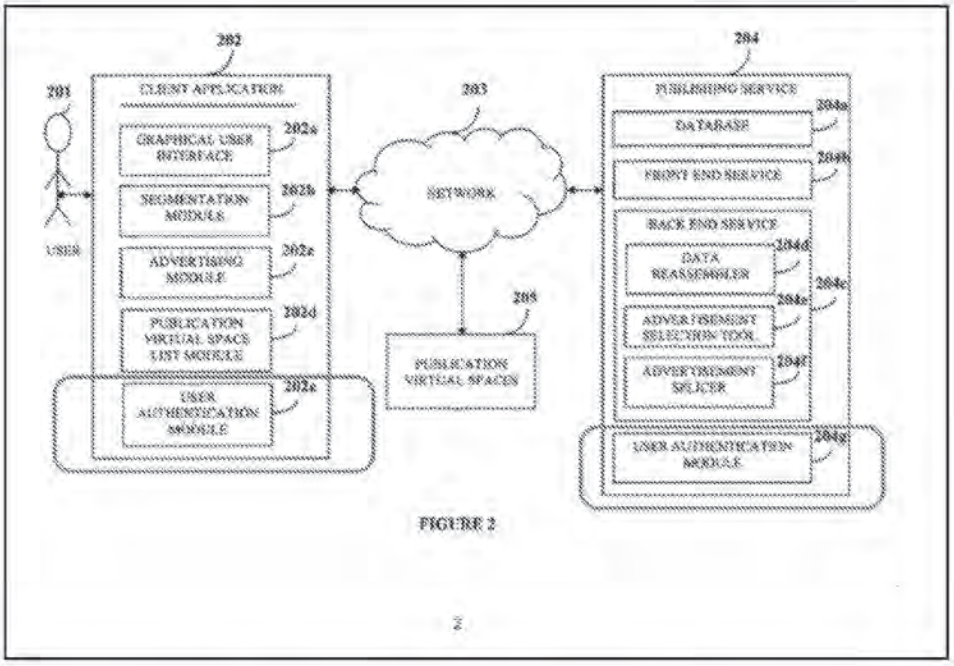


FIGURE 2

Furthermore, "Authentication" as a process step being performed in the state machine is explained in FIGURE 4 of U.S. No. 11/901,802 as highlighted above.

In response to the above rejection, applicant has amended claims 1, 4, 8 and 12, and submits that the amended claims do not contain subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention.

LifeScan, Inc. Ex. 1006
Page 291 of 353
IPR2025-00102

Furthermore, with respect to *"remains paired"* **nowhere in the specification applicant has used the word "*disconnect*" or "*unpair*" the established paired connection.** The paired connection once paired in the state machine is intended to remain paired. **There is NO mention of unpairing in the state machine of Fig 1. The "*remains paired*" is inherent in the specification and the state machine of Fig 1 because there is no unpairing.**

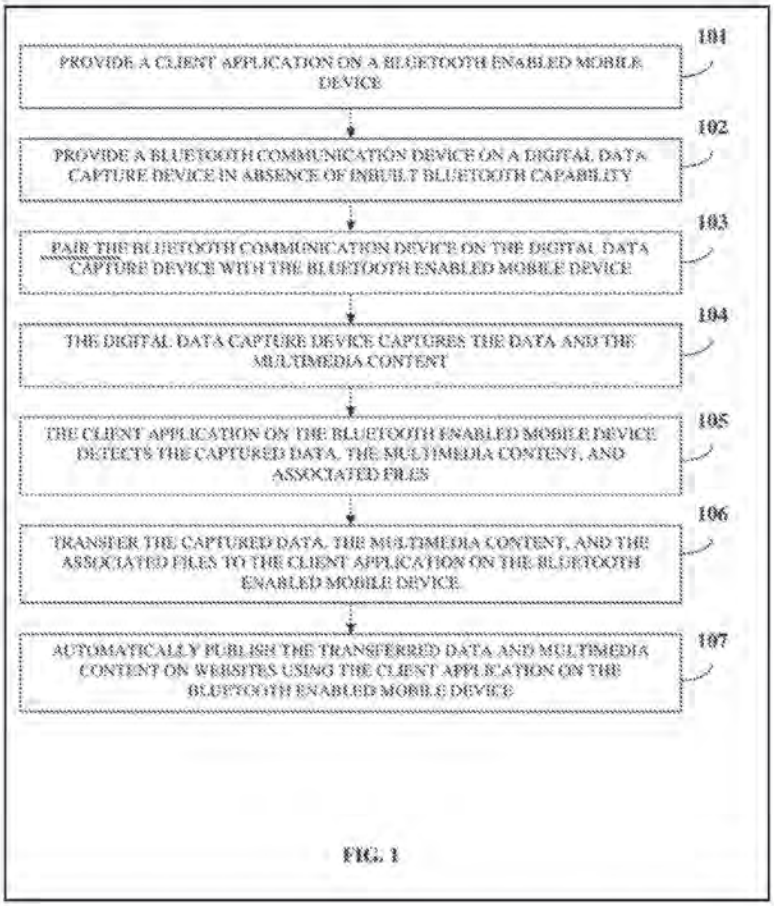


FIG. 1

Short-range Pairing and **Paired wireless connection** are terms in the art of wireless technology and has been known and was used in the wireless industry for almost 10 years before the Cellspin patent's priority date of December 2007. Bluetooth wireless standard organization was the first to introduce the term "Bluetooth" at the Blackberry

technology consortium in 1998; see Exhibit C, also available at the link: https://web.archive.org/web/20180525083558/https://www.bluetooth.com/about-us/our-history. Furthermore, in 1999, the detailed Bluetooth 1.0 specification with pairing was released; see Exhibit D attached to this response; also available at the link: http://grouper.ieee.org/groups/802/15/Bluetooth/profile_10_b.pdf.

The concept of a short-range paired connection, as established by the **Bluetooth** Special Interest Group (**Bluetooth SIG**), became known and adopted by certain other industry organizations creating wireless technology for device connections, such as WiFi Alliance and Zigbee Forum. In the context of wireless connections, the term "pairing" was adopted by the wireless industry almost 10 years before the Cellspin patent's priority date of December 2007. Drawing from wireless industry's understanding of the term "*paired wireless connection*" / pairing, the **broadest reasonable interpretation** (BRI) of "*paired wireless connection*" as understood by POSITA in Dec 2007, i.e. 10 years after the term was introduced in the wireless lexicon is:

> "bidirectional communications link between devices which provides for encrypted data exchange between the devices, and the communication link can be disconnected and reconnected without having to repeat pairing or authentication."

As explained above, POSITA understands that unless there is a specific mention of "unpair" "unpairing" the devices that are "paired" in a given state machine, those devices "remain paired" over an extended period of time. Unless and until there is an explicit call for *unpairing/unpair* the devices in that particular state machine or there is an action to remove/delete the pairing table from the device. None of applicant's state machine or the specification call for *unpairing/unpair or* remove/delete the pairing table.

Because short-range "pairing" is a well-understood term in the art, the applicant followed Federal Court's direction that the **"patent need not teach, and preferably omits, what is well known in the art."** *See McRO, Inc. v. Bandai Namco Games Am.*

Inc., 959 F.3d 1091, 1102 (Fed. Cir. 2020). In conformance with this guidance, the applicant cited a version of "pairing" at least 50 times without explicitly defining it. Additionally, while not explicitly defining "pairing," the applicant provided guidance to a POSITA that short-range "pairing" should conform to Bluetooth's conception of the term, which was later adopted when ZigBee and WiFi adopted pairing, making it the only definition applicable to short-range paired wireless connections whether or not a Bluetooth Connection.

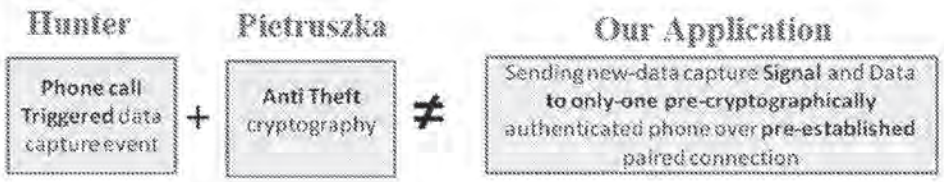
Applicant therefore respectfully requests that the rejection of claim 1 under 35 U.S.C. 112, second paragraph be reconsidered and withdrawn.

Claims 4, 8 and 12 are analogous to claim 1. Applicant therefore respectfully requests that the rejection of claims 4, 8 and 12 under 35 U.S.C. 112, second paragraph be reconsidered and withdrawn.

Claims 2-3 are dependent on claim 1. Claims 5-7 are dependent on claim 4. Claims 9-11 are dependent on claim 8. Claims 13-14 are dependent on claim 12. Applicant therefore respectfully requests that the rejection of claims 2-3, 5-7, 9-11, and 13-14 under 35 U.S.C. 112, second paragraph be reconsidered and withdrawn.

The office action further states: "**Claims 1-14 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778.**"

In response to the above rejection, applicant submits that Hunter, in view of Pietruszka does not teach or suggest all the limitations in claim 1. Furthermore, there is **no motivation** to combine (i) Phone call triggered data capture event of Hunter with (ii) the Anti-Theft Pietruszka teaching.



Arguments

Point#1: Establishment of <u>non-paired connection</u> (Hunter)

VS

Establishment of <u>paired</u> short-range Wireless (Applicant)

The office action on page 5 states that Hunter teaches the step of acquiring new-data 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. Applicant disagrees and presents the following arguments.

Hunter prior art does NOT teach pairing or paired connection. There is NO mention of word pair, pairing, paired in Hunter Specification. **Short-range Pairing** and **Paired wireless connection** are terms of short-range wireless technology and have been known and was used in the wireless industry for almost 10 years before the Cellspin patent's priority date of December 2007. Bluetooth wireless standard organization was the first to introduce the term "Bluetooth" at the Blackberry technology consortium in 1998; see Exhibit C, also available at the link: https://web.archive.org/web/20180525083558/https://www.bluetooth.com/about-us/our-history. Furthermore, in 1999, the detailed Bluetooth 1.0 specification with pairing was released; see Exhibit D attached to this response; also available at the link: http://grouper.ieee.org/groups/802/15/Bluetooth/profile_10_b.pdf.

The concept of a paired connection, as established by the **Bluetooth** Special Interest Group (**Bluetooth SIG**), became known and adopted by certain other industry organizations creating short-range wireless technology for device connections, such as

WiFi Alliance and Zigbee Forum. In the context of short-range wireless connections, the term "pairing" was adopted by the wireless industry almost 10 years before the Cellspin patent's priority date of December 2007. Drawing from short-range wireless industry's understanding of the term "*paired connection*" / pairing, the **broadest reasonable interpretation** (BRI) of "*paired connection*" as understood by POSITA in Dec 2007, i.e. 10 years after the term was introduced in the wireless lexicon is:

> "bidirectional communications link between devices which provides for encrypted data exchange between the devices, and the communication link can be disconnected and reconnected without having to repeat pairing or authentication."

Because short-range "pairing" is a well-understood term in the art, the applicant followed Federal Court's direction that the **"patent need not teach, and preferably omits, what is well known in the art."** *See McRO, Inc. v. Bandai Namco Games Am. Inc., 959 F.3d 1091, 1102 (Fed. Cir. 2020).* In conformance with this guidance, the applicant cited a version of "pairing" at least 50 times without explicitly defining it. Additionally, while not explicitly defining "pairing," the applicant provided guidance to a POSITA that short-range "pairing" should conform to Bluetooth's conception of the term, which was later adopted when ZigBee and WiFi adopted pairing, making it the only definition applicable to short-range paired wireless connections whether or not a Bluetooth Connection.

Point#2: **Receiving or making Phone call trigger event (Hunter)**

VS

NO such Phone call trigger event (Applicant)

The office action on page 6 states that Hunter teaches the step of acquiring new-data 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. Applicant disagrees and presents the following arguments.

LifeScan, Inc. Ex. 1006
Page 296 of 353
IPR2025-00102

The sequence of events in Hunter is as follows:

(i) Mobile device generates a trigger event or signal in response to a phone call received by the mobile device or a phone call made by the mobile device.

(ii) Send the trigger event or signal from the mobile device to the data capture device.

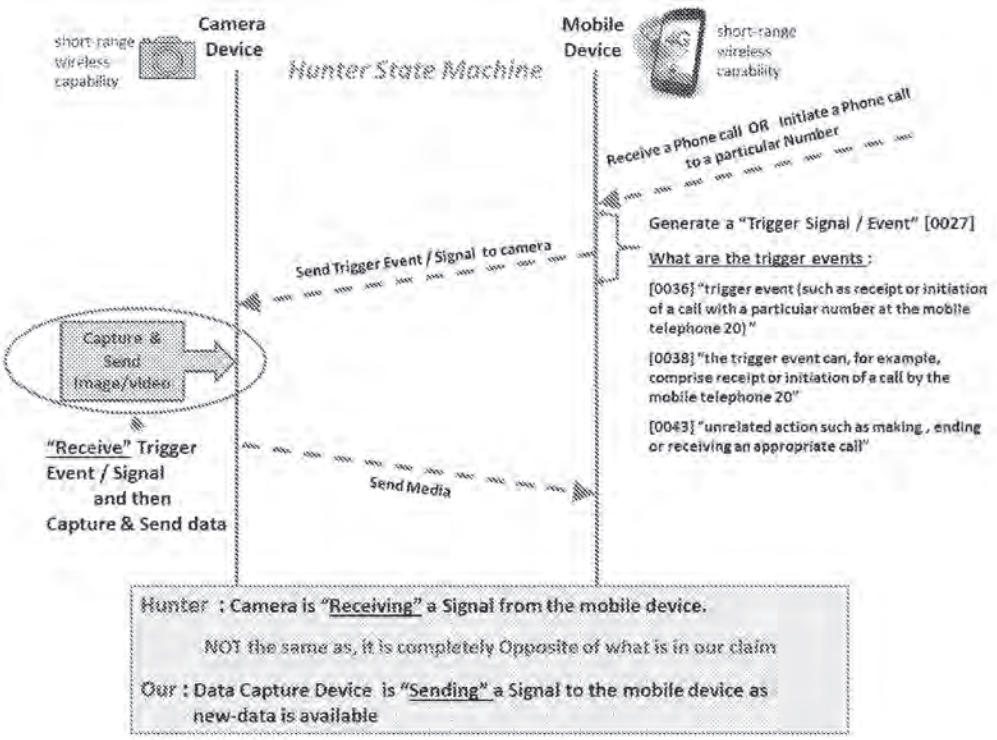
(iii) Only after receipt of the trigger event or signal from the mobile device, the data capture device acquires new-data and transmits the same to the mobile device for onward transfer to a website or web service.

Firstly, in Hunter, there is **NO pairing** of the mobile device by the data capture device. Next, there is NO cryptographic authentication of the mobile device by the data capture device. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be sent to the data capture device.

Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where a data capture device acquires new-data after a short-range paired wireless connection is established with a cellular phone (without any phone call trigger event from the cellular phone to the data capture device).

Next, **in Hunter, the phone call trigger event is sent from the mobile device to the data capture device. This is in direct contrast to applicant's disclosure,** where, after acquiring the new-data, the data capture device sends a notification signal to the mobile device informing the mobile device that it has acquired the new-data.

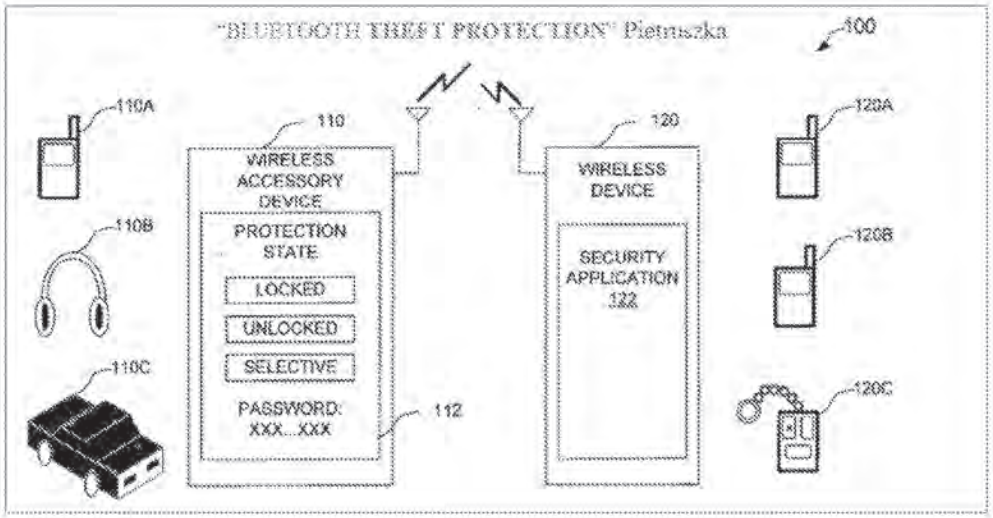
LifeScan, Inc. Ex. 1006
Page 297 of 353
IPR2025-00102



Point#3: Hunter Teaching Away from permanent paired short-range wireless connection

Hunter is teaching away from the concept of maintaining a permanent paired Bluetooth wireless connection between the camera and the mobile device (see Hunter paragraph [0009] which states as follows: "*For this reason a permanent connection to the phone is **not appropriate***," and "*It is **not easy** to maintain a voice conversation while interacting with a phone and or a camera to initiate image transfer, for example by attaching a detachable camera as described in EP-A09751342 or by configuring a Bluetooth link between a phone and a camera.*"

Point#4: Anti-Theft Pietruszka Setting based control of cryptographic pairing between devices is NOT relevant in applicant's scenario



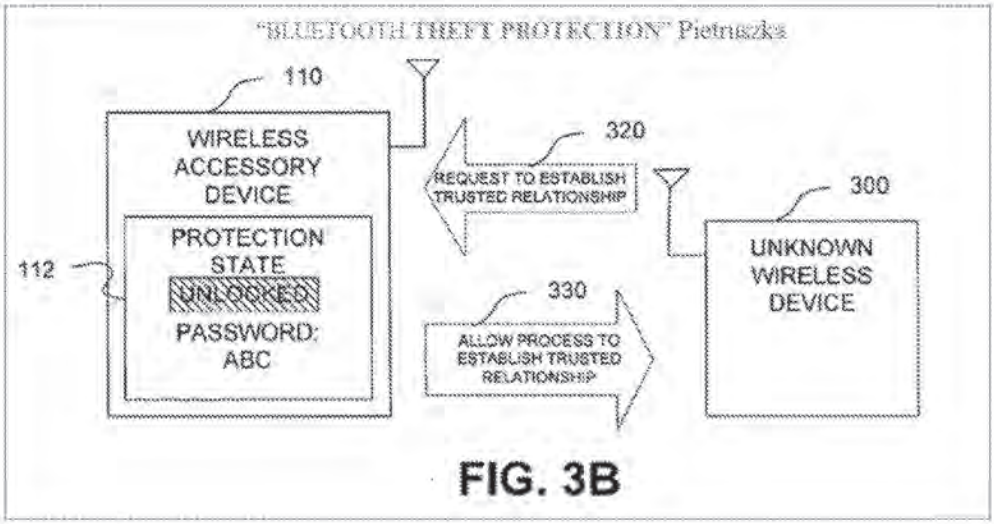


FIG. 3B

Pietruszka ("BLUETOOTH **THEFT PROTECTION**") discloses, *inter alia*, the following:

(a) User pre-selects whether or not a wireless communications device is allowed to establish a cryptographic pairing with a remote device.

LifeScan, Inc. Ex. 1006
Page 299 of 353
IPR2025-00102

(b) Control whether the wireless communications device is able to establish a cryptographic pairing with a remote device **according to the pre-set operational state**; see Pietruszka claim 1, and Paragraph [0005].

Pietruszka teaches mainly a setting-based control of cryptographic pairing between devices and it is not applicable in applicant's scenario. Applicant is NOT using a setting-based control for cryptographic pairing between devices.

Applicant is not implementing any Anti-theft technology. Applicant is not interested in a car or a key fob, or someone else hacking the car to steal it or the car accessories.

Pietruszka **teaches mainly an Anti theft technology and is not applicable in applicant's scenario. Applicant is NOT using pre-set operational state based cryptographic pairing for Anti Theft purposes for car or car accessories.**

Furthermore, in Pietruszka, **car or a key fob is "*NOT* a data capture device" and does not send any data through the mobile phone to the internet.**

In Pietruszka there is **NO** data capture device. **Car or a key fob** device described in Pietruszka is used as a *theft control device*. The **Car or a key fob** device is **NOT capturing any data for transfer through the mobile device.**

Furthermore, in Pietruszka, NO new-data is acquired for sending to the mobile phone after establishing the short-range paired wireless connection. Pietruszka's invention is all about the theft protection based on **pre-set operational state** of the device in its proximity.

Furthermore, there is NO Motivation to combine an anti theft Pietruszka with Hunter to capture data and send data to a website using a cellphone.

LifeScan, Inc. Ex. 1006
Page 300 of 353
IPR2025-00102

In view of above Points 1-4, applicant submits that Hunter, in view of Pietruszka does not teach or suggest the following limitations in amended claim 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, 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;"

> "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;"

Point#5: **Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone corresponding to the acquired new-data.**

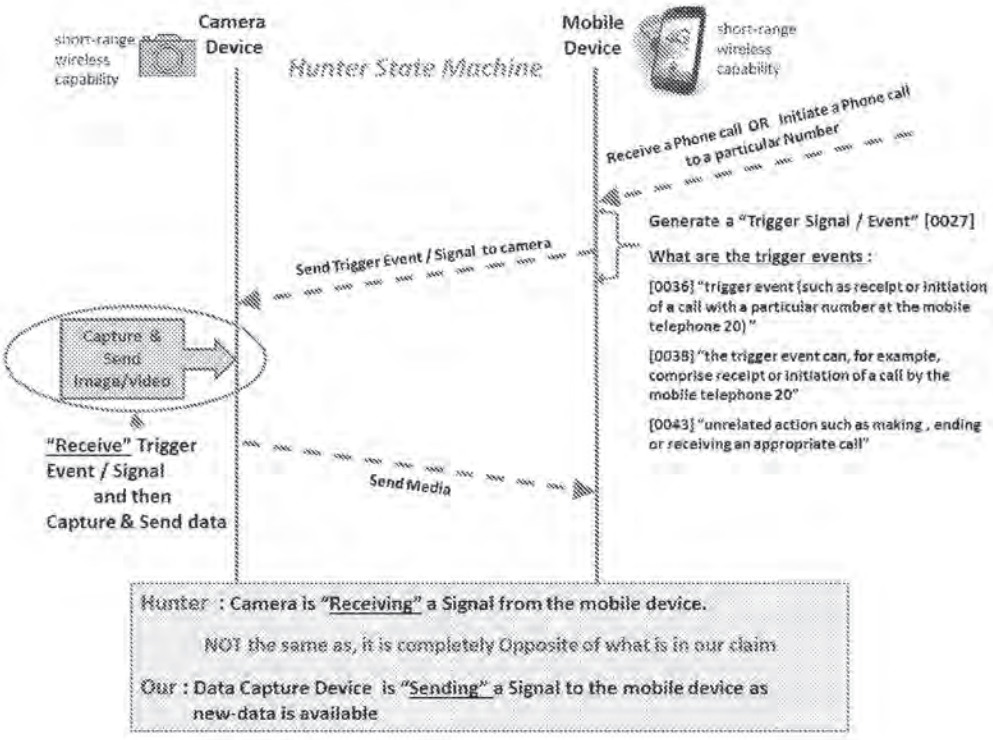
In amended claim 1, applicant discloses that after establishing the paired short-range wireless connection between the data capture device and the cryptographically authenticated short-range wireless enabled cellular phone, and after acquiring new-data, the short-range wireless enabled data capture device sends the event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone.

LifeScan, Inc. Ex. 1006
Page 301 of 353
IPR2025-00102

The office action on page 6 states that paragraph [0013] of Hunter teaches: "*Sending an event notification to a cryptographically authenticated Bluetooth enabled cellular phone*". Applicant disagrees and presents the following arguments.

Paragraph [0013] of Hunter states as follows: "*programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween; transferring images between the camera and the communications device over the wireless link; and transferring said images from the communications device on to a data network through a data network interface.*"

Hunter state machine is again reproduced below to explain paragraph [0013]:



LifeScan, Inc. Ex. 1006
Page 302 of 353
IPR2025-00102

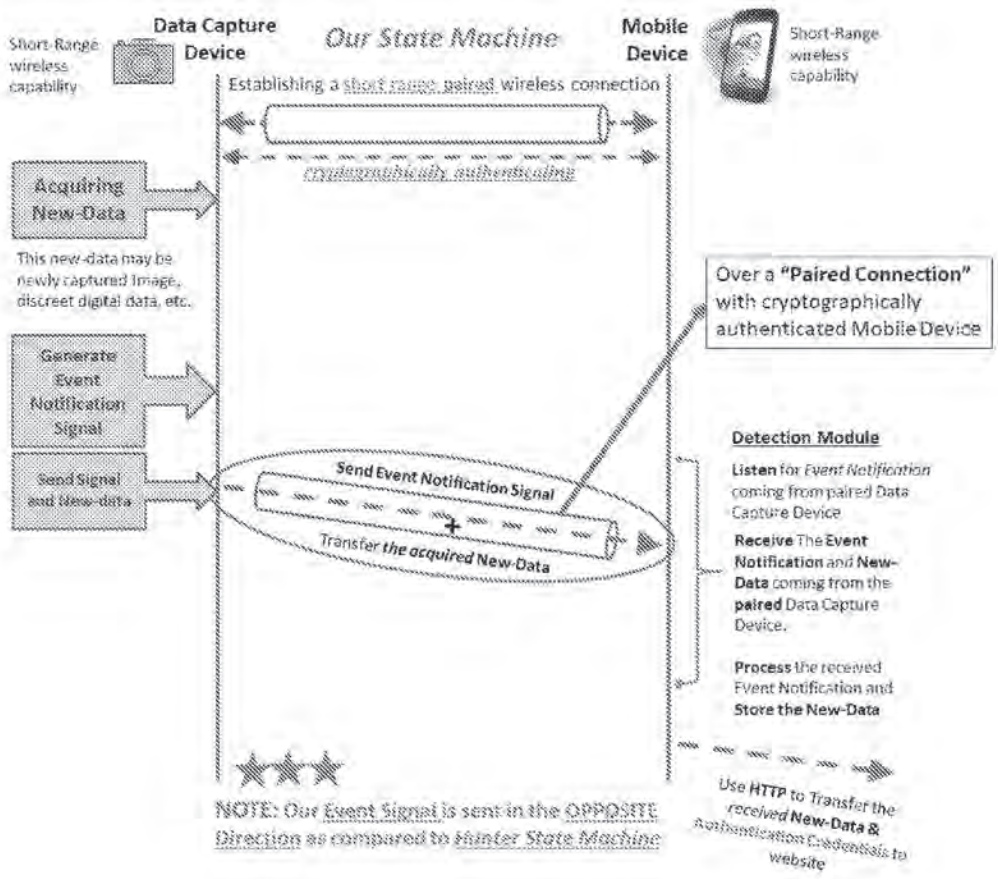
Firstly, in Hunter, there is NO cryptographic authentication of the mobile device by the data capture device before the signal is sent or the data is sent. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be sent to the data capture device.

Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. **This is in direct contrast** to applicant's disclosure where a data capture device acquires new-data after a short-range paired wireless connection is established with a cellular phone (without any phone call trigger event from the cellular phone to the data capture device).

Next, in Hunter, the phone call trigger event is sent from the mobile device to the data capture device. **Event Signal is sent in the opposite direction when compared to the applicants claims. Direction of event signal is in direct contrast to applicant's disclosure,** where, after acquiring the new-data, the data capture device sends a notification signal to the mobile device informing the mobile device that it has acquired the new-data.

In contrast, applicant's state machine is shown below.

LifeScan, Inc. Ex. 1006
Page 303 of 353
IPR2025-00102



Therefore, it is clear that the trigger notification in Hunter is not the same as the event notification in applicant's disclosure. Furthermore, in **Hunter, receipt of a phone call or an outgoing phone call is required** for the mobile device to generate the trigger event to be sent to the camera. Furthermore, in Hunter, the camera acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where the data capture device acquires new-data immediately after the paired short-range wireless connection is established (without any phone call trigger event from the mobile device). Furthermore, in Hunter, the trigger event or signal is sent from the mobile device to the camera, and image capture occurs after receiving the trigger event. **This is in direct contrast to applicant's disclosure.**

LifeScan, Inc. Ex. 1006
Page 304 of 353
IPR2025-00102

where, after acquiring the new-data, the data capture device sends the notification signal to the mobile device informing the mobile device that it has acquired the new-data.

Point#6: Phone call Trigger event in Hunter (see paragraphs [0036], [0038], [0043]) over NON paired connection

As illustrated before, in Hunter, there is no cryptographic authentication of the mobile device by the camera. Furthermore, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate the trigger event or signal to be sent to the camera. Furthermore, in Hunter, the camera acquires the new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where the data capture device acquires the new-data immediately after a paired short-range wireless connection is established (without any phone call trigger event from the mobile device). Furthermore, in Hunter, the phone call trigger event or signal is sent from the mobile device to the camera. This is in direct contrast to applicant's disclosure, where, after acquiring the new-data, the data capture device sends the notification signal and the acquired new-data to the mobile device.

Point#7: Use HTTP to transfer new-data and a user authentication credential to website

In applicant's invention, the cellular phone uses HTTP to transfer new-data and a user authentication credential to website. Neither Hunter nor Pietruszka teach or suggest the use of HTTP to transfer the new-data and the user authentication credential to the website.

In view of above Points 5-7, applicant submits that Hunter, in view of Pietruszka does not teach or suggest the following limitation in amended claim 1:

"said processor further configured to send an event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled

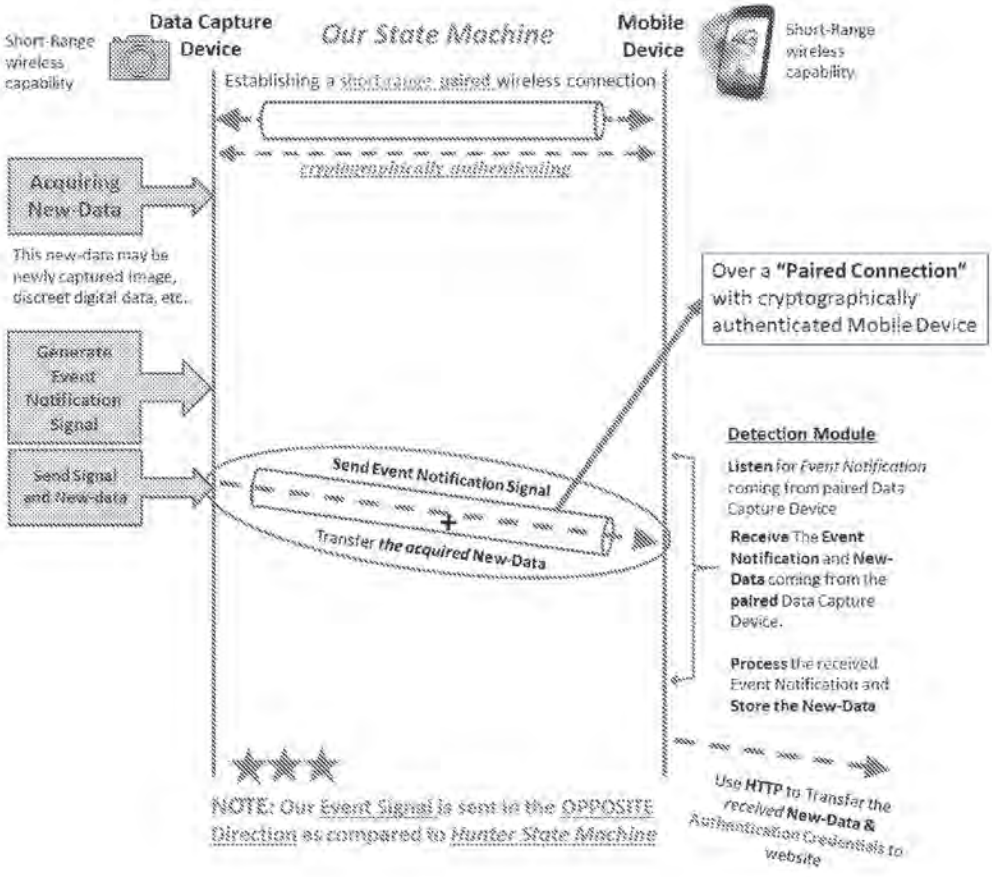
LifeScan, Inc. Ex. 1006
Page 305 of 353
IPR2025-00102

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, 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, wherein a 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, 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 and a user authentication credential to a user data publishing website over a cellular data network."

LifeScan, Inc. Ex. 1006
Page 306 of 353
IPR2025-00102

Summary

Applicant's state machine



LifeScan, Inc. Ex. 1006
Page 307 of 353
IPR2025-00102

Comparison Table

	Claim Feature	Hunter	Pietruszka	Applicant Cellspin
1	Pairing for new data transfer.	NO mention of pairing. Pairing is NOT established. Teaching away from establishing permanent connection.	NO Invention is about selecting or preventing, and controlling pairing between devices. NOT for new data transfer	YES Pairing is established to transfer the acquired new data.
7	Cryptographically authenticate the identity of Mobile Device	NO	YES Only if wireless communication device is unlocked for pairing.	YES The Mobile device is cryptographically authenticated by the data capture device NOT based on pre-selection of activation or deactivation of pairing.
3	Sending new data capture Event Notification Signal	NO Trigger Event Signal is sent from the mobile device to the camera device, which is opposite to applicant's invention.	NO There is NO data capture Event signal sent to the cellular phone. There is NO data capture device.	YES Event Notification signal is sent from data capture device to cellular phone after acquiring new data.
4	Send data to the mobile device over a pre-established paired connection	NO	NO There is no data to transfer.	YES
4	HTTP based transfer	NO HTTP is NOT used.	NO There is No data to transfer.	YES HTTP is used as a data transport protocol.
5	Is Timing of Data Acquisition after Pairing devices	NO	NO	YES After pairing is established.
6	Data transfer between two devices happens over what type of wireless link?	NON-Paired wireless connection	NO data There is no new data to transfer.	Data over Paired wireless connection

In view of the above arguments, state machines and illustrative drawings, applicant submits that amended claim 1 is non-obvious over Hunter, in view of Pietruszka. Claims 4, 8 and 12 are analogous to claim 1, and include all the limitations of amended claim 1. Therefore, claims 4, 8 and 12 are also non-obvious over Hunter, in view of Pietruszka. Claims 2-3 are dependent on amended claim 1; claims 5-7 are dependent on amended claim 4; claims 9-11 are dependent on amended claim 8; claims 13-14 are dependent on amended claim 12. Applicant therefore submits that dependent claims 2-3, 5-7, 9-11, and 13-14 are also non-obvious over Hunter, in view of Pietruszka.

Applicant therefore respectfully requests that the rejection of claims 1-14 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

LifeScan, Inc. Ex. 1006
Page 308 of 353
IPR2025-00102

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case. In the interest of compact prosecution, if the prosecution of the application can be advanced, applicant requests Examiner Nooristany to call the undersigned with the proposed amendment.

Respectfully submitted,

Date: October 16, 2020

/a tankha/
Ashok Tankha
Attorney For Applicant
Reg. No. 33,802

Correspondence Address
Lipton Weinberger & Husick
36 Greenleigh Drive
Sewell, NJ 08080
Phone: 856-266-5145
Email: ash@ipprocurement.com

LifeScan, Inc. Ex. 1006
Page 309 of 353
IPR2025-00102

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/532,507	08/06/2019	Gurvinder Singh	CellSpin_04Con17_US	6207

7590 07/17/2020

Ashok Tankha
36 Greenleigh Drive
Sewell, NJ 08080

EXAMINER	
NOORISTANY, SULAIMAN	

ART UNIT	PAPER NUMBER
2415	

MAIL DATE	DELIVERY MODE
07/17/2020	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

LifeScan, Inc. Ex. 1006
Page 310 of 353
IPR2025-00102

Office Action Summary	Application No. 16/532,507	Applicant(s) Singh et al.	
	Examiner SULAIMAN NOORISTANY	Art Unit 2415	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 8/6/19.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-14 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-14 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. More specifically, the applicant fails to sufficiently point out or describe

cellular phone remains paired after storing the created new-data;

wherein the user preferences comprise authentication credentials and global positioning system information.

The specification of this application under examination does not contain subject matter to implement limitations, as cited in the following claims.

Claim 1 recites newly presented claim limitation

Also, it is not apparent how "***remains paired***" & "***authentication credentials and global positioning system information***" is determined.

LifeScan, Inc. Ex. 1006
Page 312 of 353
IPR2025-00102

Examiner has reviewed the specification of this application under examination (and OCR whole document) and could not find support for the additional limitations as claimed.

Specification Objection

The disclosure is objected to because of the following informalities: Examiner has reviewed the specification of this application under examination and could not find support for the additional limitations as claimed "***remains paired***" & "***authentication credentials & global positioning system information***". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 1-14 are rejected under 112, second paragraph as being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention

In claim **4**, the terms "***remains paired***" & "***authentication credentials" and "global positioning system information***" are not clear what these are in reference to. Also, the description of the present application fails to provide a clear and complete description on the invention as well as the above terms. However, the claims will be given a broad reasonable interpretation for the purposes of examination as best understood.

Claims 1-3, 5-14 are rejected for similar reasons as stated for claim 4.

LifeScan, Inc. Ex. 1006
Page 313 of 353
IPR2025-00102

Claim Rejections - 35 USC § 103

In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1-14 is/are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778.

4. A system, comprising:

a short-range wireless enabled data capture device **(Hunter fig. 1, unit 10)**, comprising:

a first memory device **(Hunter: a camera with an image memory and a first wireless communication interface [0010] fig. 1, unit 10)**;

a first processor coupled to the first memory device **(Hunter: a camera with an image memory and a first wireless communication interface [0010] fig. 1, unit 10)**;

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 **(Hunter: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10 to establish a data link between the two units. Alternatively, the camera 10 may**

LifeScan, Inc. Ex. 1006
Page 314 of 353
IPR2025-00102

periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10 [0017-0027, 0036-0037]).

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;

a data capture circuitry **(Hunter: fig. 1 unit 10)**;

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 **(Hunter: [0017-0027, 0036-0037] After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038])**;

said first processor further configured to store the new-data in the first memory device **(Hunter: After the data link is established, the camera 10 can transmit (via the wireless communication link 16), in response to a trigger event, video or still image data representative of images stored in or being captured thereby, either continuously or periodically, for receipt by the mobile telephone [0038])**, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the created new-data **(Hunter: [0017-0027, 0036-0038] The wireless link may be pre-existing, or may be set up only on the initiation of the call [0039-0040])**; and

LifeScan, Inc. Ex. 1006
Page 315 of 353
IPR2025-00102

said first processor further configured to send an event notification **(Hunter: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween [0013])** and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically **(Hunter: transferring images between the camera and the communications device over the wireless link [0013])**;

said short-range wireless enabled cellular phone **(Hunter: fig. 1 unit 20)**, comprising:

a second memory device **(Hunter: fig. 1 unit 20)**;

a second processor coupled to the second memory device **(Hunter: fig. 1 unit 20)**;

a cellular network communication device configured to connect to the internet via the cellular data network **(Hunter: fig. 1 unit 20)**;

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 **(Hunter: when the mobile telephone is switched on, it may transmit a signal for receipt and acknowledgement by the camera 10 to establish a data link between the two units. Alternatively, the camera 10 may periodically transmit a signal which is received and acknowledged by the mobile telephone 20 to establish a data link between the two units when it is switched on and/or comes within a predetermined distance of the camera 10 [0017-0027, 0036-0037])**;

a mobile client application for the short-range wireless enabled cellular phone comprising executable instructions that, when executed by the second processor controls the second

LifeScan, Inc. Ex. 1006
Page 316 of 353
IPR2025-00102

processor to: listen for an event notification sent by the short-range wireless enabled data capture device, wherein a mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the event notification (**Hunter: programming a camera and a communications device to recognize a trigger event; one of the camera and the communications device recognizing occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween [0013]**);

receive the new-data from the short-range wireless enabled data capture device (**Hunter: an image storage buffer 24 for storing image data received from the camera 10 [0035]**);

store the received new-data in the second memory device (**Hunter: an image storage buffer 24 for storing image data received from the camera 10 [0035]**), wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the received new-data (**Hunter: The wireless link may be pre-existing, or may be set up only on the initiation of the call [0017-0027, 0036-0037, 0039-0040]**); and

use HTTP to upload the received new-data and user publication information to a user data publishing website over the cellular data network, wherein the user publication information comprises user preferences, and wherein the user preferences comprise authentication credentials and global positioning system information (**Hunter: transferring said images from the communications device on to a data network through a data network interface [0013, 0035, 0041]**).

Hunter merely discloses the term *cryptographically* authenticating

LifeScan, Inc. Ex. 1006
Page 317 of 353
IPR2025-00102

Pietruszka further teaches cryptographically authenticating (**Pietruszka: [0037]**) in order to communicate only with a trusted device can cryptographically authenticate the identity of the other device.

Thus, it would have been obvious to one skill in the art to include the above recited limitation into Hunter's in order to communicate only with a trusted device can cryptographically authenticate the identity of the other device [0037], as taught by Pietruszka.

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 **(Hunter: [0037])**

6. 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 **(Hunter: [0020])**

7. The system of claim 4, 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 **(Hunter: [0020])**

Regarding claims 1-3, 8-14 the independent claim and each dependent claim are related to the same limitation set for hereinabove in claims 4-7, where the difference used is a "capture device" & "mobile device" and the wordings of the claims were interchanged within the claim itself or some of the claims were presented as a combination of two or more previously presented limitations. This change does not affect the limitation of the above treated claims. Adding these

LifeScan, Inc. Ex. 1006
Page 318 of 353
IPR2025-00102

phrases to the claims and interchanging the wording did not introduce new limitations to these claims. Therefore these claims were rejected for similar reasons as stated above

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sulaiman Nooristany whose telephone number is 571-270-1929. The examiner can normally be reached on Monday thru Friday: 8:30am to 5:00pm (EST). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Rutkowski can be reached on 571-270-1215. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/SULAIMAN NOORISTANY/

Primary Examiner, Art Unit 2415

LifeScan, Inc. Ex. 1006
Page 319 of 353
IPR2025-00102

AUTOMATIC MULTIMEDIA UPLOAD FOR PUBLISHING DATA AND MULTIMEDIA CONTENT

CROSS REFERENCE TO RELATED APPLICATIONS

1. This application is a continuation application of non-provisional patent application number 15/659,637, titled "Automatic multimedia upload for publishing data and multimedia content", filed July 26, 2017 in the United States Patent and Trademark Office, which is a continuation application of non-provisional patent application number 14/576,202, now patent 9,749,847, titled "Automatic multimedia upload for publishing multimedia content", filed December 19, 2014 in the United States Patent and Trademark Office, which is a continuation application of non-provisional patent application number 14/503,401, titled "Automatic multimedia upload for publishing multimedia content", filed October 01, 2014 in the United States Patent and Trademark Office, which is a continuation application of non-provisional patent application number 14/273,546, now Patent no. 8,862,757, titled "Automatic multimedia upload for publishing multimedia content", filed May 09, 2014 in the United States Patent and Trademark Office, which is a continuation application of non-provisional patent application number 14/172,913, now Patent no. 8,798,539, titled "Automatic multimedia upload for publishing multimedia content", filed on February 05, 2014 in the United States Patent and Trademark Office, which is a continuation application of non-provisional patent application number 13/740,214, now Patent no. 8,700,790, titled "Automatic multimedia upload for publishing multimedia content", filed on January 13, 2013 in the United States Patent and Trademark Office, which is a continuation application of non-provisional patent application number 12/333,303, now Patent no. 8392591, titled "Automatic multimedia upload for publishing multimedia content", filed on December 11, 2008 in the United States Patent and Trademark Office, which claims the benefit of US provisional patent application number 61/017,202, titled "Automatic multimedia upload for publishing multimedia content", filed on December 28, 2007 in the United

LifeScan, Inc. Ex. 1006
Page 320 of 353
IPR2025-00102

States Patent and Trademark Office. The specifications of the above referenced applications are incorporated herein by reference in their entirety.

2. The following patent application is incorporated herein in its entirety: US Non-provisional patent application serial number 11/901,802, titled "Online Publishing of Multimedia Content", filed on September 19, 2007 in the United States Patent and Trademark Office.

BACKGROUND

This invention, in general, relates to distribution of multimedia content. More particularly, this invention relates to pairing a digital data capture device in conjunction with a mobile device for automatically publishing data and multimedia content on one or more websites simultaneously.

A user may need to capture and publish data and multimedia content on the internet in real time. Typically, the user would capture an image using a digital camera or a video camera, store the image on a memory device of the digital camera, and transfer the image to a computing device such as a personal computer (PC). In order to transfer the image to the PC, the user would transfer the image off-line to the PC, use a cable such as a universal serial bus (USB) or a memory stick and plug the cable into the PC. The user would then manually upload the image onto a website which takes time and may be inconvenient for the user.

Therefore, there is a need for a method and system to utilize a digital data 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 or with minimal user intervention.

SUMMARY OF THE INVENTION

LifeScan, Inc. Ex. 1006
Page 321 of 353
IPR2025-00102

This summary is provided to introduce a selection of concepts in a simplified form that are further described in the detailed description of the invention. This summary is not intended to identify key or essential inventive concepts of the claimed subject matter, nor is it intended for determining the scope of the claimed subject matter.

The method and system disclosed herein addresses the above stated need 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. The digital data capture device is physically separated from the BT enabled mobile device.

In the method and system disclosed herein, a client application is provided on a BT enabled mobile device. In the absence of in-built BT capability in the digital data capture device, a BT communication device is provided on the digital data capture device. The BT communication device may, for example, be an in-built BT capability chip, a BT memory card, or an external BT device. The BT communication device on the digital data capture device is paired with the BT enabled mobile device to establish a connection between the digital data capture device and the BT enabled mobile device.

A user may capture data and multimedia content using the digital data capture device. The digital data capture device may, for example, be a digital camera, a video camera, or other digital modular camera systems. The client application on the BT enabled mobile device detects the captured data, multimedia content, and files associated with the captured data and the multimedia content on the digital data capture device by communicating over a wireless BT protocol. The captured data, multimedia content, and the associated files are automatically transferred to the client application on the BT enabled mobile device from the digital data capture device.

The detection and transfer of the captured data, the multimedia content, and the associated files may be initiated by the client application of the BT enabled mobile

LifeScan, Inc. Ex. 1006
Page 322 of 353
IPR2025-00102

device. The detection and transfer of the captured data, the multimedia content, and the associated files to the BT enabled mobile device may be initiated by the digital data capture device when the client application is unable to detect the captured data, the multimedia content, and the associated files from the digital data capture device.

The user may configure a timer setting and select the websites for publishing using the client application on the BT enabled mobile device. The client application selects the websites for publishing the transferred data and the multimedia content based on user preferences configured on the Bluetooth enabled mobile device. The client application also sets time for publishing the transferred data and the multimedia content automatically or with minimal user intervention. The client application on the BT enabled mobile device automatically publishes the transferred data and multimedia content on one or more websites using the settings configured by the user. 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. The user may therefore publish data and the multimedia content on immediate capture of the data and the multimedia content on the digital data capture device.

The method and system disclosed herein is described with reference to a BT communication protocol. The method and system disclosed herein may be realized with wireless protocols, for example, Zigbee® protocol, Wibree™ protocol, Ultra-Wide Band (UWB) protocol, and other wireless protocols for wireless personal area networks.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing summary, as well as the following detailed description of the invention, is better understood when read in conjunction with the appended drawings. For the purpose of illustrating the invention, exemplary constructions of the invention are

shown in the drawings. However, the invention is not limited to the specific methods and instrumentalities disclosed herein.

FIG. **1** illustrates a method of utilizing a digital data capture device in conjunction with a Bluetooth enabled mobile device for publishing data and multimedia content on one or more websites automatically or with minimal user intervention.

FIG. **2** illustrates a system for utilizing a digital data capture device in conjunction with a Bluetooth enabled mobile device for publishing data and multimedia content on one or more websites automatically or with minimal user intervention.

FIGS. **3A-3C** exemplarily illustrate the Bluetooth communication device options used on the digital data capture device for establishing a Bluetooth connection with the client application on the Bluetooth enabled mobile device.

FIG. **4** exemplarily illustrates a system for publishing data and the multimedia content using a client application on a mobile device on one or more websites simultaneously.

FIG. **5** exemplarily illustrates a user utilizing a digital camera in conjunction with a Bluetooth enabled mobile device for publishing data and multimedia content on one or more websites automatically or with minimal user intervention.

DETAILED DESCRIPTION OF THE INVENTION

FIG. **1** illustrates a method of utilizing a digital data capture device **201** in conjunction with a Bluetooth™ enabled mobile device **202** for publishing data and multimedia content on one or more websites automatically or with minimal user intervention. The term "Bluetooth enabled mobile device" is herein referred to as "mobile device". The digital data capture device **201** is physically separated from the mobile device **202** as illustrated in FIG. **2**. The digital data capture device **201** may, for example,

LifeScan, Inc. Ex. 1006
Page 324 of 353
IPR2025-00102

be a digital camera, a video camera, digital modular camera systems, or other digital data capturing systems.

In the method disclosed herein, a client application **203** is provided **101** on the mobile device **202**. In the absence of inbuilt Bluetooth (BT) capability in the digital data capture device **201**, a BT communication device **201a** is provided **102** on the digital data capture device **201**. The BT communication device **201a** may, for example, be an inbuilt BT capability chip **301**, a BT memory card **302**, or an external BT device **303** as illustrated in FIGS. **3A-3C** respectively. The external BT device **303** may, for example, be attached to a universal serial bus (USB), a firewire interface, or a power port of the digital data capture device **201**. BT provides a method of connecting and exchanging information between devices, for example, mobile phones, laptops, personal computers (PCs), printers, digital cameras, etc. over a secure and globally unlicensed short-range radio frequency.

The BT communication device **201a** on 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**. BT pairing involves establishing a connection between two BT devices that mutually agree to communicate with each other. A BT device that wants to communicate only with a trusted device can cryptographically authenticate the identity of another BT device. BT pairing occurs when the BT communication device **201a** agrees to communicate with the mobile device **202** in order to establish a connection. In order to initiate the pairing process between the BT communication device **201a** and the mobile device **202**, a common password known as a passkey is exchanged between the BT communication device **201a** and the mobile device **202**. A passkey is a code shared by the BT communication device **201a** and the mobile device **202**.

A user sets a discoverable mode for the mobile device **202**. When set to the discoverable mode, the mobile device **202** will allow the BT communication device **201a** on the digital data capture device **201** to detect the mobile device's **202** presence and

LifeScan, Inc. Ex. 1006
Page 325 of 353
IPR2025-00102

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

The user captures **104** data and multimedia content using the digital data capture device **201**. The data and multimedia content may, for example, comprise image files, audio files, video files, text files, or any combination thereof. The client application **203** on the mobile device **202** detects **105** the captured data, the multimedia content, and files associated with the captured data and the multimedia content. The client application **203** then initiates the transfer of the captured data, the multimedia content, and the associated files in a pull mode of operation. 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. The file transfer protocols may, for example, be one or a combination of BT profile protocols such as the object exchange (OBEX) protocol, the generic object exchange profile (GOEP) protocol, etc. The file transfer protocols may, for example, also be the media transfer protocol (MTP), the picture transfer protocol (PTP), and the PictBridge protocol implemented using a USB.

The picture transfer protocol (PTP) allows the transfer of images from digital cameras to computers and other peripheral devices without the need of additional device drivers. The media transfer protocol is a custom extension to the PTP and allows the protocol to be used for devices other than digital cameras, for example digital audio

LifeScan, Inc. Ex. 1006
Page 326 of 353
IPR2025-00102

players and other portable media devices, for example portable video players. The PictBridge protocol allows images to be printed directly from digital cameras to a printer, without having to connect the camera to a computer.

The transfer of the data, the multimedia content, and the associated files may also take place in a push mode of operation. 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**. For some external digital data capture devices, the client application **203** may not be able to detect the creation of a new file. In such cases, the digital data capture device **201** signals the client application **203** in the event a new file is created. 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**.

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. The data segments are tagged with segment identifiers using the client application **203**. 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**.

When the client application **203** is unable to detect the captured data, the multimedia content, and the associated files from the digital data capture device **201**, the digital data capture device **201** initiates detection and transfer of the captured data, the multimedia content, and the associated files to the mobile device **202**.

The user may also set preferences on the mobile device **202**. The user preferences may, for example, comprise the websites selected for publishing the data and the multimedia content. The user may configure a timer setting and the websites on the

LifeScan, Inc. Ex. 1006
Page 327 of 353
IPR2025-00102

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. The user may set the timer setting to, for example, a "no-wait-automatic" setting, a "wait-X-minutes-automatic" setting, and a "wait-X-minutes-user-input-cancel" setting. The client application **203** on the mobile device **202** selects the websites for publishing the transferred data and the multimedia content based on user preferences configured on the mobile device **202**. The client application **203** also sets time for publishing the transferred data and the multimedia content automatically or with minimal user intervention.

The client application **203** on the mobile device **202** then automatically publishes **107** the transferred data and multimedia content on one or more websites. If the user configures the timer setting to "no-wait-automatic", the data and the multimedia content are automatically published on one or more websites based on the user preferences configured on the mobile device **202** without waiting for a certain period of time. If the user configures the timer setting to "wait-X-minutes-automatic", the client application **203** will wait for "X" minutes for the user to change or cancel publishing. If there is no user action for "X" minutes, the client application **203** will automatically publish the data and multimedia content to one or more websites based on the user preferences. Further, if the user configures the timer setting to "wait-X-minutes-user-input-cancel", the client application **203** will wait for "X" minutes for an input from the user. If there is no input from the user, the client application **203** cancels the publishing of the data and multimedia content. The publishing of the data and multimedia content on one or more websites simultaneously is explained in the detailed description of FIG. **4**.

The user may therefore capture data, for example, audio, video, text, and images, automatically upload the captured data onto the mobile device **202**, and publish the data and multimedia content on one or websites automatically or with minimal user intervention. The method disclosed herein thereby enables the user to publish data and the multimedia content on immediate click of an image or recording of a video on the digital data capture device **201** without having to manually upload the data onto a computing device and then publish the data on the websites.

FIG. **2** illustrates a system for utilizing a digital data capture device **201** in conjunction with a BT enabled mobile device **202** for publishing data and multimedia content on one or more websites automatically or with minimal user intervention. The system disclosed herein comprises a digital data capture device **201** and a client application **203** provided on the BT enabled mobile device **202**. The digital data capture device **201** and the mobile device **202** are physically separated from each other. The digital data capture device **201** comprises a BT communication device **201a** and a data capture module **201d**.

The BT communication device options used on the digital data capture device **201** for establishing a BT connection with the client application **203** on the BT enabled mobile device **202** are exemplarily illustrated in FIGS. **3A-3C**. The BT communication device **201a** may, for example, be an in-built BT capability chip **301** as illustrated in FIG. **3A**, a BT memory card **302** as illustrated in FIG. **3B**, or an external BT device **303** as illustrated in FIG. **3C**.

The BT communication device **201a** comprises a BT association protocol module **201b** and a data transfer protocol module **201c**. 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**. 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**. The pairing of the BT communication device **201a** and the mobile device **202** is explained in the detailed description of FIG. **1**. The data capture module **201d** captures the data and the multimedia content on the digital data capture device **201**.

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**. When the client application **203** is unable to detect the captured data, the multimedia content, and the associated files from the digital data capture device **201**, the data transfer protocol module **201c** of the digital data capture device **201** initiates the transfer of the captured data, the multimedia content, and the associated files to the mobile device **202**.

The data transfer protocol module **201c** of the digital data capture device **201** transfers the captured data, the multimedia content, and the associated files to the client application **203**. The data storage module **203d** stores the captured data, the multimedia content, and the associated files on the mobile device **202**. 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**. The user may set a timer setting, for example, a "no-wait-automatic" setting, a "wait-X-minutes-automatic" setting, and a "wait-X-minutes-user-input-cancel" setting as explained in the detailed description of FIG. **1**.

The media publishing module **203f** automatically publishes the transferred data and the multimedia content on one or more of the websites. The media publishing module **203f** comprises a website selection module **203g**, a timer module **203h**, a segmentation module **203i**, and a data transfer module **203j**. The website selection module **203g** selects the websites for publishing the data and the multimedia content based on settings and user preferences configured by the user on the mobile device **202**. The timer module **203h** sets the time for publishing the transferred data and the multimedia content automatically or with minimal user intervention. The timer setting may be set for automatic publishing of the multimedia content or a time based wait mode where user

interaction is required. The timer module **203h** sets the timer based on a timer setting, for example, a "no-wait-automatic" setting, a "wait-X-minutes-automatic" setting, and a "wait-X-minutes-user-input-cancel" setting configured by the user. The timer module **203h** ensures that if the user does not wish to publish the transferred data and multimedia content, the user has time to decide whether to publish or not. The user may also configure the client application **203** to automatically delete the data, the multimedia content, and the associated files after the data and the multimedia content have been posted and published on one or more websites based on user preferences.

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**. The segmentation module **203i** generates segment identifiers and tags the data segments with the segment identifiers. The data transfer module **203j** transfers the data, the tagged data segments, and the multimedia content from the client application **203** to the publishing service **401** via a network **402** for publishing on the websites automatically.

FIG. **4** exemplarily illustrates a system for publishing data and the multimedia content using a client application **203** on a mobile device **202** on one or more websites simultaneously. The system disclosed herein comprises a client application **203** and a publishing service **401** connected via a network **402**. The client application **203** comprises a media publishing module **203f** as explained in the detailed description of FIG. **2**. The media publishing module **203f** comprises the website selection module **203g**, the timer module **203h**, the segmentation module **203i**, and the data transfer module **203j**. The website selection module **203g** selects the websites based on user preferences configured by the user on the mobile device **202**. The timer module **203h** sets the time for publishing the transferred data and the multimedia content automatically or with minimal user intervention. The timer module **203h** ensures that the publishing service **401** obtains the data, the multimedia content, and the associated files to publish on the selected websites based on the time set by the user.

In the case of limited memory and processing capabilities of the mobile device **202**, the segmentation module **203i** of the client application **203** partitions the multimedia content of large files into multiple data segments. The segmentation module **203i** 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. The segment identifiers are used later by a back end service **401b** of the publishing service **401** to reassemble the data segments in a predetermined sequence to create a multimedia object. The data transfer module **203j** 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**.

The publishing service **401** comprises a front end service **401a**, a back end service **401b**, and a database **401d**. The transferred data and multimedia content is stored in the database **401d** of the publishing service **401**. A protocol is provided for synchronizing user publishing information between the client application **203** and the publishing service **401**. The user publishing information may, for example, comprise user preferences of the websites and the timer setting. The data transfer module **203j** may transfer the data and the multimedia content as a single multimedia file, multiple data segments in the case of large files, or electronic mail attachments to the back end service **401b** of the publishing service **401** via the front end service **401a**. The back end service **401b** comprises a data reassembly module **401c**. 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. The back end service **401b** then creates a multimedia object from the transferred data and multimedia content. The multimedia object is transferred from the back end service **401b** to the front end service **401a** and then published on the websites selected by the user.

FIG. **5** exemplarily illustrates a user **502** utilizing a digital camera in conjunction with a Bluetooth enabled mobile device **202** for publishing data and multimedia content

LifeScan, Inc. Ex. 1006
Page 332 of 353
IPR2025-00102

on one or more websites automatically or with minimal user intervention. The digital camera is physically separated from the mobile device **202** as illustrated in FIG. **5**. The digital camera comprises a BT communication device **201a** such as an in-built BT capability chip **301**, a BT memory card **302**, or an external BT device **303** or dongle externally attached to the digital camera as illustrated in FIGS. **3A-3C**. The external BT dongle may be attached to a USB, a firewire interface, or a power port of the digital camera. The BT communication device **201a** on the digital camera is paired with the mobile device **202** to establish a connection. The user **502** may capture an image using the digital camera. The client application **203** on the mobile device **202** detects the captured image and initiates the transfer of the captured image and the associated files. The digital camera automatically transfers the captured image and the associated files to the client application **203** on the mobile device **202**.

The client application **203** automatically publishes the transferred image on one or more websites via the internet **501**. The user **502** may set preferences in the mobile device **202**. The user preferences, for example, comprise the websites selected for publishing the transferred image. The user **502** may select websites, for example, Flickr™, Picasa™, YouTube™, eBay®, etc. and store the preferences on the mobile device **202**. The user **502** may also set the timer setting for publishing the transferred image on the selected websites. After the captured image is transferred to the mobile device **202**, the client application **203** publishes the capture image on the selected websites based on the default timer and website settings configured by the user **502** on the mobile device **202**.

Consider an example where a user **502** records a video using a BT enabled video camera. The video camera immediately establishes a connection with the user's **502** BT enabled mobile device **202**. On detection of the recorded video by the client application **203** on the mobile device **202**, the video camera automatically transfers the recorded video to the user's **502** mobile device **202**. In the case of limited memory and processing capabilities of the mobile device **202**, the recorded video may be streamed as data segments from the mobile device **202** to the publishing service **401**. The client

application **203** individually tags the data segments with segment identifiers and transfers the tagged data segments from the mobile device **202** to the back end service **401b** of the publishing service **401** via the front end service **401a**. The back end service **401b** of the publishing service **401** reassembles the data segments in a predetermined sequence using the segment identifiers to create the multimedia object. The multimedia object is an aggregation of the reassembled data segments. The multimedia object is then transferred from the back end service **401b** to the front end service **401a** and automatically published by the front end service **401a** on one or more websites selected by the user **502**.

Consider another example where a user **502** may record videos or capture images at different points in time and automatically uploads and publishes the videos and images on one or more websites. Consider an investigative reporter, Jane, working for a prominent newspaper in New York City. Each day, she moves around the city chasing leads, interviewing people, videotaping her stories, taking pictures, and tracking down her next big story. When she is working on a story with an associate writer, she may need to upload her videos and pictures and send it immediately to the associate writer. The method and system disclosed herein enables Jane to automatically upload pictures and videos taken using her digital camera or video camera onto a mobile device **202** and publish the pictures, videos, etc. from her mobile device **202** to the internet **501** with one click or touch of a button.

On one click or touch of a button, the pictures and videos are published and immediately made available on Jane's private blog that may be accessed by the newspaper editor and her associates in the news office. When she is collaborating with an associate on a story, they may see each other's progress in real time. Since sharing information with the associate over electronic mails (emails) may be inconvenient, Jane records her progress on the story in the voice format and publishes. The associate may access the information from Jane's blog site, thereby saving considerable time.

Exemplarily, the method and system disclosed herein may be implemented in technologies that are pervasive, flexible, and capable enough of accomplishing the

LifeScan, Inc. Ex. 1006
Page 334 of 353
IPR2025-00102

desired tasks of the method and system. The method and system disclosed herein is realized with, but not limited to Bluetooth communication protocol. Wireless protocols, for example, Zigbee® protocol, Wibree™ protocol, Ultra-Wide Band (UWB) protocol, and other wireless protocols for wireless personal area networks may be employed to accomplish the tasks of the method and system disclosed herein. The mobile device **202** may, for example, be a ubiquitous mobile phone. The use of personal digital assistants (PDAs) without telephony support is also fairly widespread. The client application **203** may be deployed on mobile devices with limited or no telephony support. These mobile devices may support Java of Sun Microsystems Inc., more specifically Java 2 Micro Edition (J2ME™), Windows Mobile .Net Compact Framework of Microsoft, Inc., Symbian™, Linux framework. The client application **203** may, for example, be implemented on the J2ME platform. These environments provide functionalities in the libraries to create the GUI **203e** and perform all the required functions of the method and system disclosed herein. Other advantages of these frameworks are portability across mobile devices that run on different operating systems.

The client application **203** may be rendered independent of the operating system of the mobile device **202**. One of the transport mechanisms to achieve the connectivity between the publishing service **401** and the client application **203** is the wireless internet. While most PDAs have an inbuilt wireless network card for the internet connectivity, the mobile phones may transfer data to the publishing service **401** over the telephony network at near broadband speeds. Some of the mobile phones equipped with both wireless network and telephony data capabilities may use either of the two to communicate with the publishing service **401**. The transport protocol that is used between the client application **203** and the publishing service **401** may be hypertext transfer protocol (HTTP) or extensible markup language-remote procedure calls (XML-RPC). The back end service **401b** may, for example, be developed in Java.

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.,

LifeScan, Inc. Ex. 1006
Page 335 of 353
IPR2025-00102

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. Further, programs that implement such methods and algorithms may be stored and transmitted using a variety of media, for e.g., computer readable media in a number of manners. In one embodiment, hard-wired circuitry or custom hardware may be used in place of, or in combination with, software instructions for implementation of the processes of various embodiments. Thus, embodiments are not limited to any specific combination of hardware and software. A "processor" means any one or more microprocessors, Central Processing Unit (CPU) devices, computing devices, microcontrollers, digital signal processors or like devices. The term "computer-readable medium" refers to any medium that participates in providing data, for example instructions that may be read by a computer, a processor or a like device. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media include, for example, optical or magnetic disks and other persistent memory volatile media include Dynamic Random Access Memory (DRAM), which typically constitutes the main memory. Transmission media include coaxial cables, copper wire and fiber optics, including the wires that comprise a system bus coupled to the processor. Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, any other magnetic medium, a Compact Disc-Read Only Memory (CD-ROM), Digital Versatile Disc (DVD), any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a Random Access Memory (RAM), a Programmable Read Only Memory (PROM), an Erasable Programmable Read Only Memory (EPROM), an Electrically Erasable Programmable Read Only Memory (EEPROM), a flash memory, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read. In general, the computer-readable programs may be implemented in any programming language. Some examples of languages that can be used include C, C++, C#, or JAVA. The program will use various security, encryption and compression techniques to enhance the overall user experience. The software programs may be stored on or in one or more mediums as an object code. A computer program product comprising computer executable instructions embodied in a

LifeScan, Inc. Ex. 1006
Page 336 of 353
IPR2025-00102

computer-readable medium comprises computer parsable codes for the implementation of the processes of various embodiments.

Where databases are described such as the database **401d**, it will be understood by one of ordinary skill in the art that (i) alternative database structures to those described may be readily employed, and (ii) other memory structures besides databases may be readily employed. Any illustrations or descriptions of any sample databases presented herein are illustrative arrangements for stored representations of information. Any number of other arrangements may be employed besides those suggested by, e.g., tables illustrated in drawings or elsewhere. Similarly, any illustrated entries of the databases represent exemplary information only; one of ordinary skill in the art will understand that the number and content of the entries can be different from those described herein. Further, despite any depiction of the databases as tables, other formats including relational databases, object-based models and/or distributed databases could be used to store and manipulate the data types described herein. Likewise, object methods or behaviors of a database can be used to implement various processes, such as the described herein. In addition, the databases may, in a known manner, be stored locally or remotely from a device that accesses data in such a database.

The present invention can be configured to work in a network environment including a computer that is in communication, via a communications network, with one or more devices. The computer may communicate with the devices directly or indirectly, via a wired or wireless medium such as the Internet, Local Area Network (LAN), Wide Area Network (WAN) or Ethernet, Token Ring, or via any appropriate communications means or combination of communications means. Each of the devices may comprise computers, such as those based on the Intel® processors, AMD® processors, Sun® processors, IBM® processors etc., that are adapted to communicate with the computer. Any number and type of machines may be in communication with the computer.

The foregoing examples have been provided merely for the purpose of explanation and are in no way to be construed as limiting of the present method and

LifeScan, Inc. Ex. 1006
Page 337 of 353
IPR2025-00102

system disclosed herein. While the invention has been described with reference to various embodiments, it is understood that the words, which have been used herein, are words of description and illustration, rather than words of limitation. Further, although the invention has been described herein with reference to particular means, materials and embodiments, the invention is not intended to be limited to the particulars disclosed herein; rather, the invention extends to all functionally equivalent structures, methods and uses, such as are within the scope of the appended claims. Those skilled in the art, having the benefit of the teachings of this specification, may effect numerous modifications thereto and changes may be made without departing from the scope and spirit of the invention in its aspects.

LifeScan, Inc. Ex. 1006
Page 338 of 353
IPR2025-00102

Claims

We Claim:

1. A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

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;

a data capture circuitry;

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;

said processor further configured to store the new-data in the memory device, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the created new-data;

LifeScan, Inc. Ex. 1006
Page 339 of 353
IPR2025-00102

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, 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, wherein a 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, 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 and user publication information to a user data publishing website over a cellular data network, wherein the user publication information comprises user preferences, and wherein the user preferences comprise authentication credentials and global positioning system information.

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. A system, comprising:

a short-range wireless enabled data capture device, comprising:

a first memory device;

LifeScan, Inc. Ex. 1006
Page 340 of 353
IPR2025-00102

a first processor coupled to the first memory device;

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;

a data capture circuitry;

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;

said first processor further configured to store the new-data in the first memory device, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the created new-data; and

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;

said short-range wireless enabled cellular phone, comprising:

LifeScan, Inc. Ex. 1006
Page 341 of 353
IPR2025-00102

a second memory device;

a second processor coupled to the second memory device;

a cellular network communication device configured to connect to the internet via the cellular data network;

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;

a 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 an event notification sent by the short-range wireless enabled data capture device, wherein a mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the event notification;

receive the new-data from the short-range wireless enabled data capture device;

store the received new-data in the second memory device, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the received new-data; and

LifeScan, Inc. Ex. 1006
Page 342 of 353
IPR2025-00102

use HTTP to upload the received new-data and user publication information to a user data publishing website over the cellular data network, wherein the user publication information comprises user preferences, and wherein the user preferences comprise authentication credentials and global positioning system information.

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 new-data comprises one or more of audio data, video data, image data, text data, digital data, and data associated with the new-data.

7. The system of claim 4, 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.

8. A short-range wireless enabled cellular phone, comprising:

a memory device;

a processor coupled to the memory device;

a cellular network communication device configured to connect to internet via a cellular data network;

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;

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:

listen for an event notification sent by the short-range wireless enabled data capture device;

receive the event notification and the new-data from the short-range wireless enabled data capture device;

process the event notification and store the received new-data in the second memory device, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the received new-data; and

use HTTP to upload the received new-data and user publication information to a user data publishing website over the cellular data network, wherein the user publication information comprises user preferences, and wherein the user preferences comprise authentication credentials and global positioning system information.

9. The short-range wireless enabled cellular phone of claim 8, 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.

10. The short-range wireless enabled cellular phone of claim 8, 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.

11. The short-range wireless enabled cellular phone of claim 8, 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.

12. A short-range wireless enabled data capture device, comprising:

a memory device;

a processor coupled to the memory device;

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;

a data capture circuitry;

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

LifeScan, Inc. Ex. 1006
Page 345 of 353
IPR2025-00102

short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;

said processor further configured to store the new-data in the memory device of the short-range wireless enabled data capture device, wherein the established short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone remains paired after storing the created new-data;

said processor further configured to listen to a polling request from a mobile client application on the cryptographically authenticated short-range wireless enabled cellular phone, over the established paired short-range wireless connection, wherein the polling request is for the new-data, wherein the mobile client application on the cryptographically authenticated 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 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 mobile client application on the cryptographically authenticated short-range wireless enabled cellular phone, over the established paired short-range wireless connection;

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 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 mobile client application on the

LifeScan, Inc. Ex. 1006
Page 346 of 353
IPR2025-00102

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 mobile client application on the short-range wireless enabled cellular phone is further configured to use HTTP to upload the received new-data and user publication information to a user data publishing website over a cellular data network, wherein the user publication information comprises user preferences, and wherein the user preferences comprise authentication credentials and global positioning system information.

13. The short-range wireless enabled data capture device of claim 12, 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.

14. The short-range wireless enabled data capture device of claim 12, 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.

LifeScan, Inc. Ex. 1006
Page 347 of 353
IPR2025-00102

ABSTRACT

Disclosed herein is a method and system for utilizing a digital data capture device in conjunction with a Bluetooth (BT) enabled mobile device for publishing data and multimedia content on one or more websites automatically or with minimal user intervention. A client application is provided on the BT enabled mobile device. In the absence of inbuilt BT capability, a BT communication device is provided on the digital data capture device. The BT communication device is paired with the BT enabled mobile device to establish a connection. The client application detects capture of data and multimedia content on the digital data capture device and initiates transfer of the captured data, multimedia content, and associated files. The digital data capture device transfers the captured data, multimedia content, and the associated files to the client application. The client application automatically publishes the transferred data and multimedia content on one or more websites.

LifeScan, Inc. Ex. 1006
Page 348 of 353
IPR2025-00102

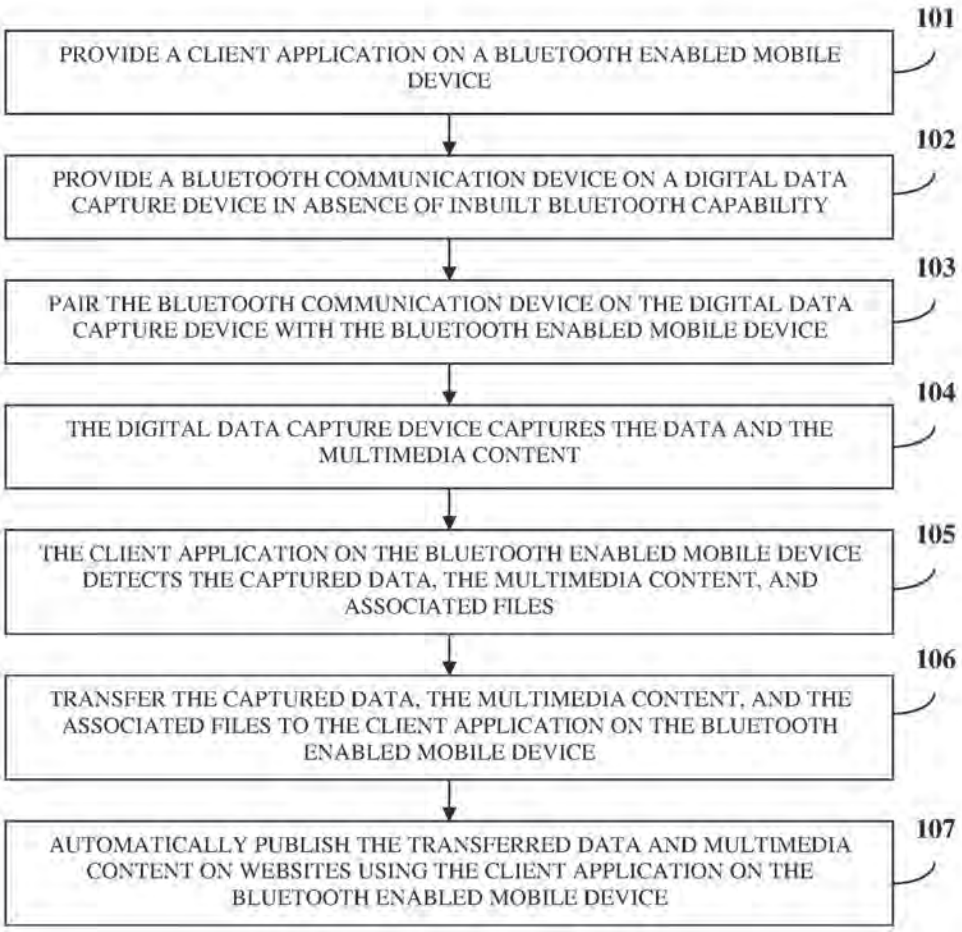


FIG. 1

LifeScan, Inc. Ex. 1006
Page 349 of 353
IPR2025-00102

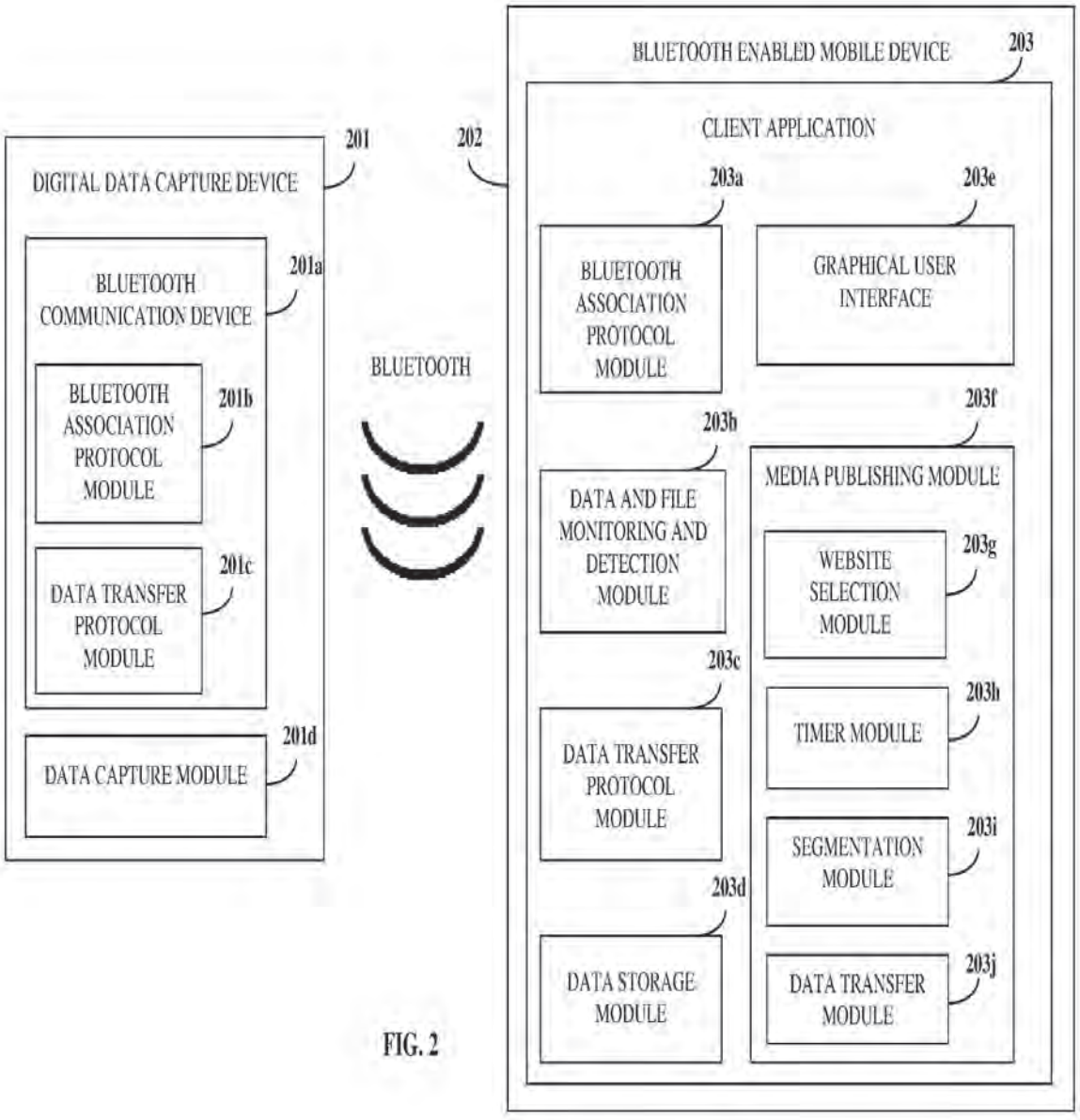


FIG. 2

LifeScan, Inc. Ex. 1006
Page 350 of 353
IPR2025-00102

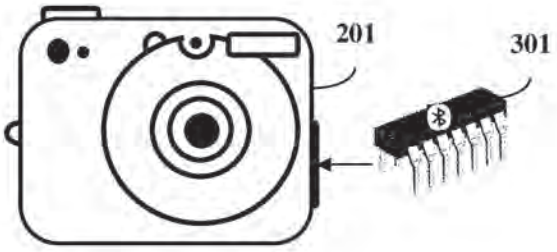


FIG. 3A

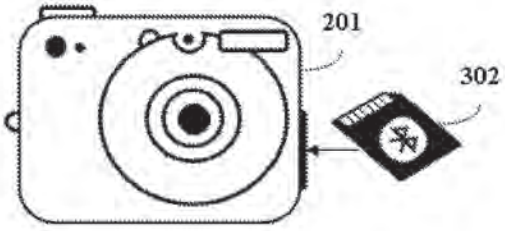


FIG. 3B

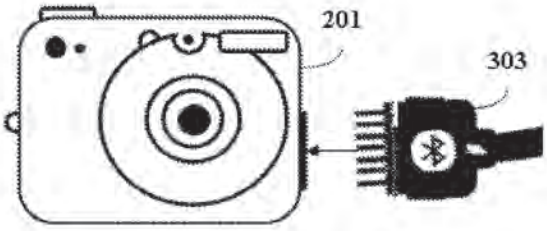


FIG. 3C

LifeScan, Inc. Ex. 1006
Page 351 of 353
IPR2025-00102

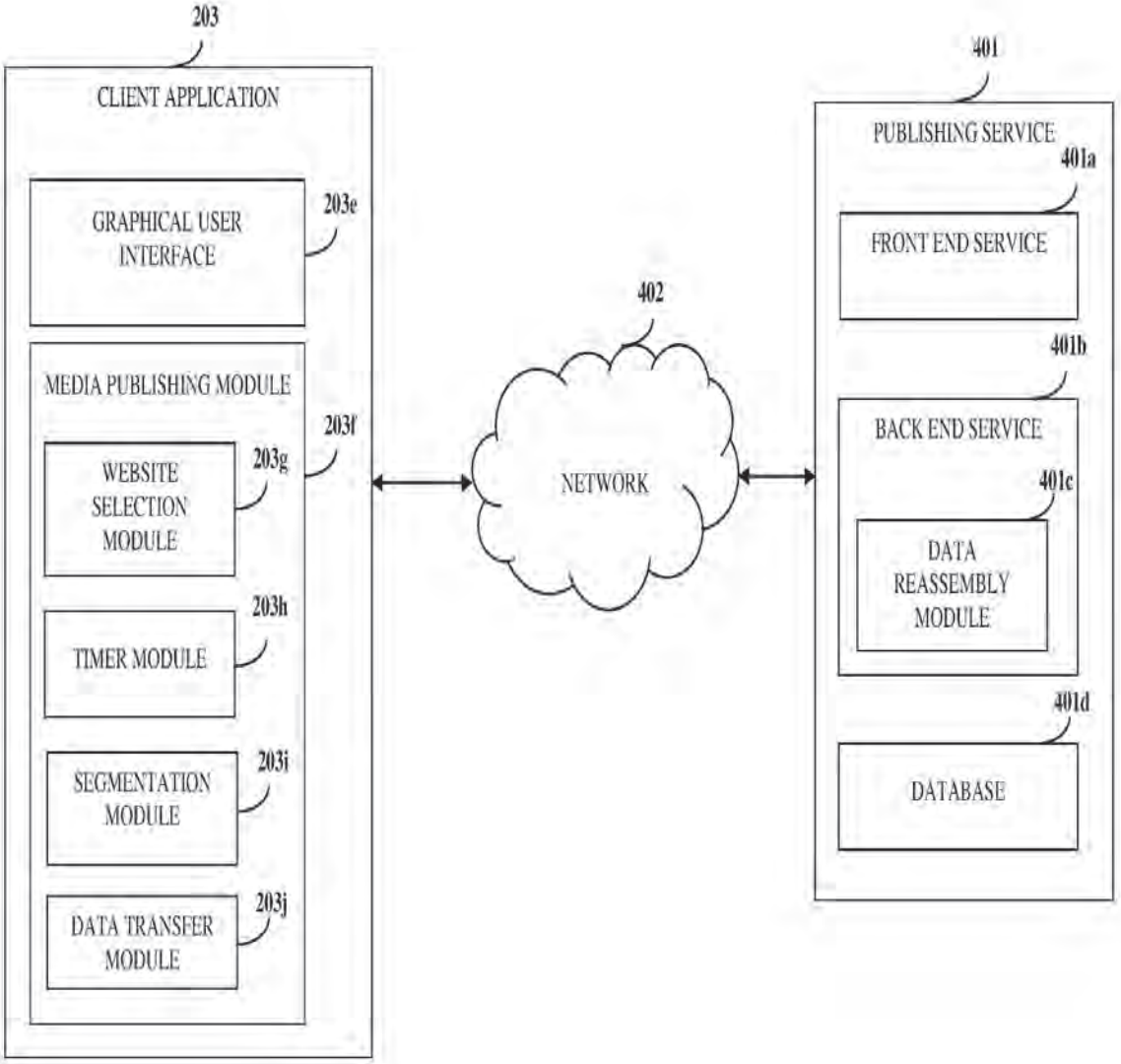


FIG. 4

LifeScan, Inc. Ex. 1006
Page 352 of 353
IPR2025-00102

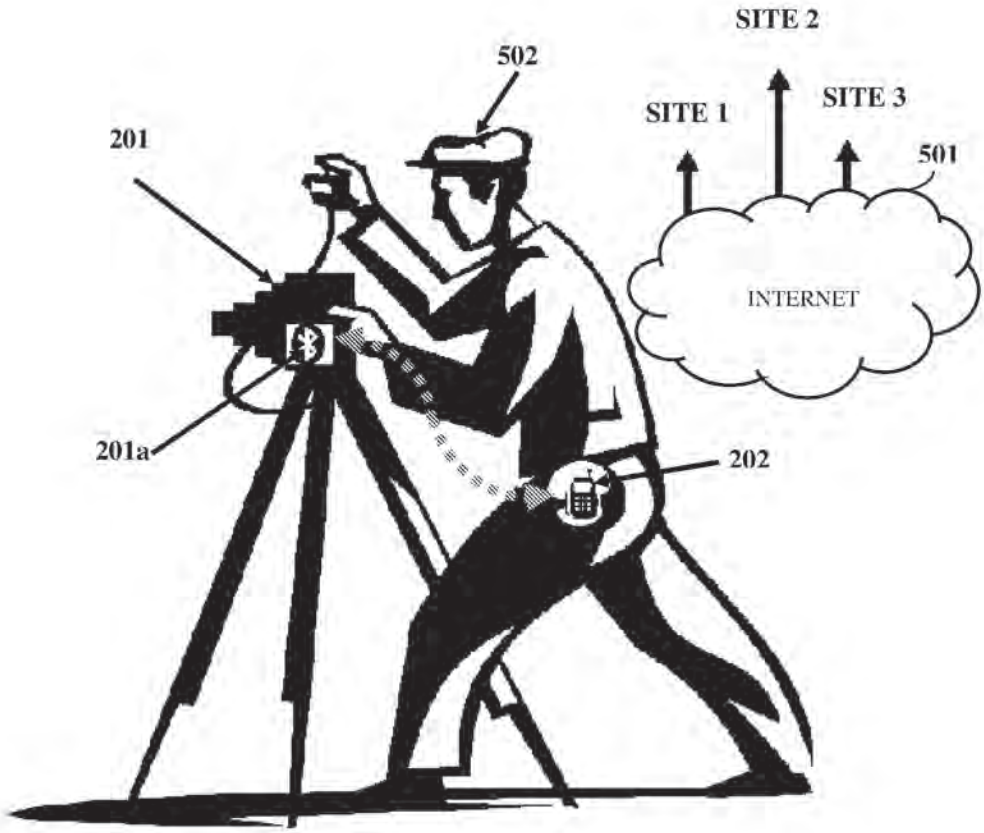


FIG. 5

LifeScan, Inc. Ex. 1006
Page 353 of 353
IPR2025-00102