



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)

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.

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

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,

1 _____

(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.

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	EXAMINER	
ASHOK TANKHA 36 GREENLEIGH DRIVE SEWELL, NJ 08080			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.

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.

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. <u>9/3/21</u> .	5. ☐ Examiner's Amendment/Comment 6. ☐ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____.
---	---

/SULAIMAN NOORISTANY/
Primary Examiner, Art Unit 2415

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

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

Date of Interview: 03 September 2021

Issues Discussed:

Proposed Amendment(s)

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

/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: It is not necessary for applicant to provide a separate record of the substance of 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.

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

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.

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

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[,] 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;

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;

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,

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).

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.

Date: September 6, 2021

Correspondence Address

Respectfully submitted,

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re. application of:

Gurvinder Singh

Application No.: 16/532,507

Filed: 08/06/2019

Applicant: Cellspinsoft Inc.

Title: Automatic Multimedia Upload

For Publishing Data And Multimedia Content

Examiner: Nooristany, Sulaiman

Art Unit: 2415

Atty. Docket no.: CellSpin_04Con17_US

Mail Stop Amendment

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Preliminary Amendment

Examiner Nooristany:

In response to the advisory action mailed July 29, 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

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;

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.

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

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;

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;

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, 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.

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

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

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.”*

- (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**

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.”

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**”.

- (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**”.

(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

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

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”.

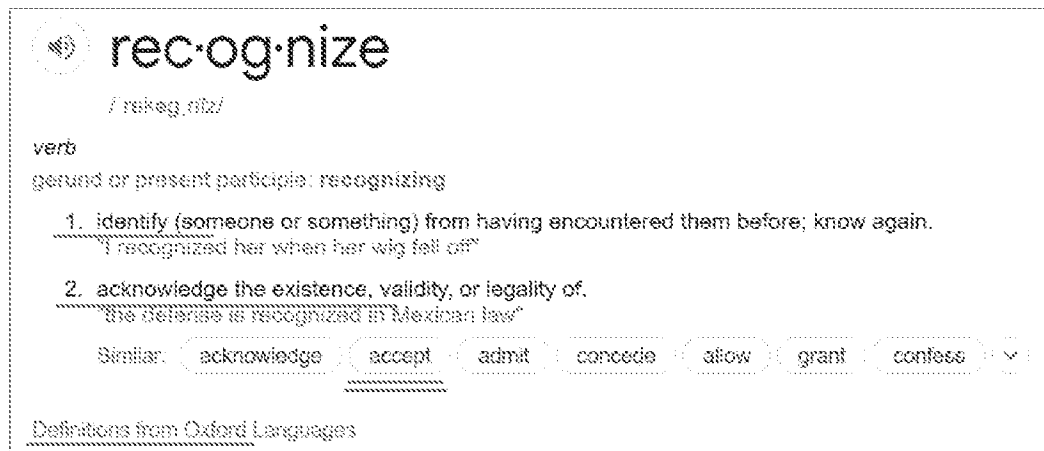
Applicant respectfully *disagrees* and submits the following arguments:

Hunter [0013]

[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 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.

Recognizing $\neq$ Sending

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



rec·og·nize
 /ˈreɪk.ə.naɪz/
 verb
 gerund or present participle: recognizing

1. identify (someone or something) from having encountered them before; know again.
 "I recognized her when her wig fell off"
2. acknowledge the existence, validity, or legality of.
 "the detente is recognized in Mexican law"

Similar: acknowledge, accept, admit, concede, allow, grant, confess

Definitions from Oxford Languages

(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:

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:

provide a touch based graphical user interface for the received new-data (Hunter: [0025], Pietruszka [0099])	
Hunter [0025] In any event, once a data link has been established, the image capture device may be arranged to periodically transmit a frame of image data to the mobile telephone to be transmitted, stored or discarded, according to whether or not the mobile telephone user actually wishes to transmit image data at that time. In a preferred embodiment, the mobile telephone may comprise a selection switch which, when actuated, causes image data to be selectively stored or transmitted across the telephone network. Thus, if the selection switch is not actuated, no image data is stored or transmitted, and image data (if any) sent from the image capture device to the mobile telephone is discarded. Alternatively or additionally, there may be a means to activate storage or transmission of images to a mobile telephone as a result of an operation of the camera, such as a touch or voice command.	Pietruszka [0099] 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 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.
➤ In Hunter [0025] the touch interface and operation is on the Camera device and for the image taken on/by the camera. ➤ In our claims the touch interface is on the Mobile device and is for the image received from the camera. ➤ Two completely different devices and for two completely different reasons.	➤ In Pietruszka [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. ➤ In our claims the touch based user interface is for the “received new-data”

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.

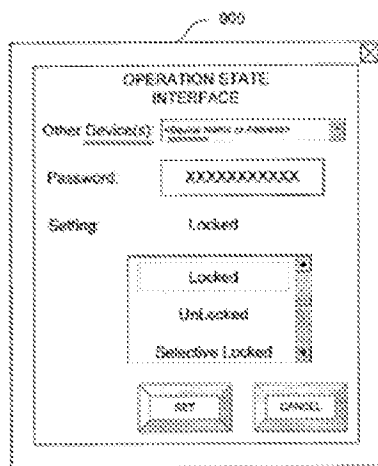


FIG. 9A

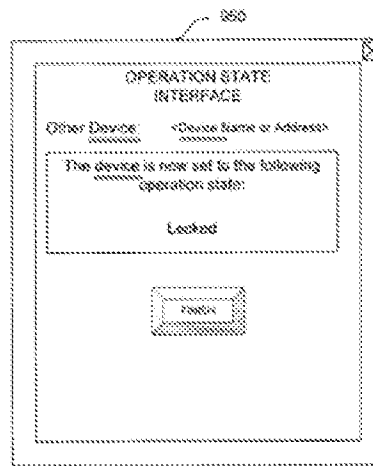


FIG. 9B

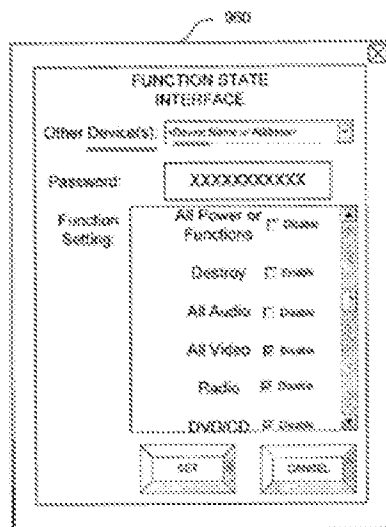


FIG. 9C

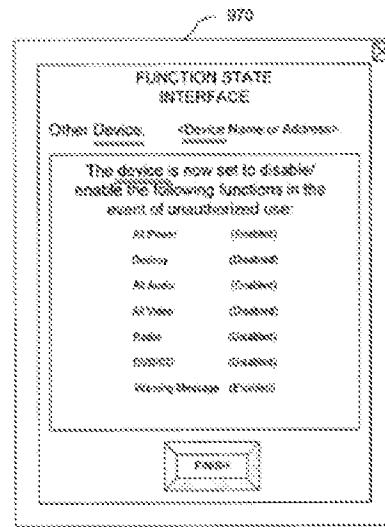


FIG. 9D

- 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

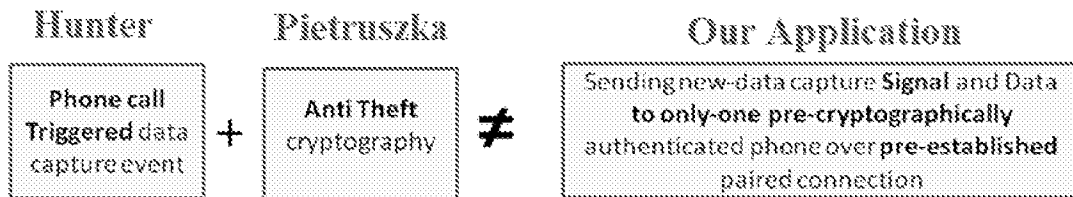
Cryptographic authentication of a wireless device

≠

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.

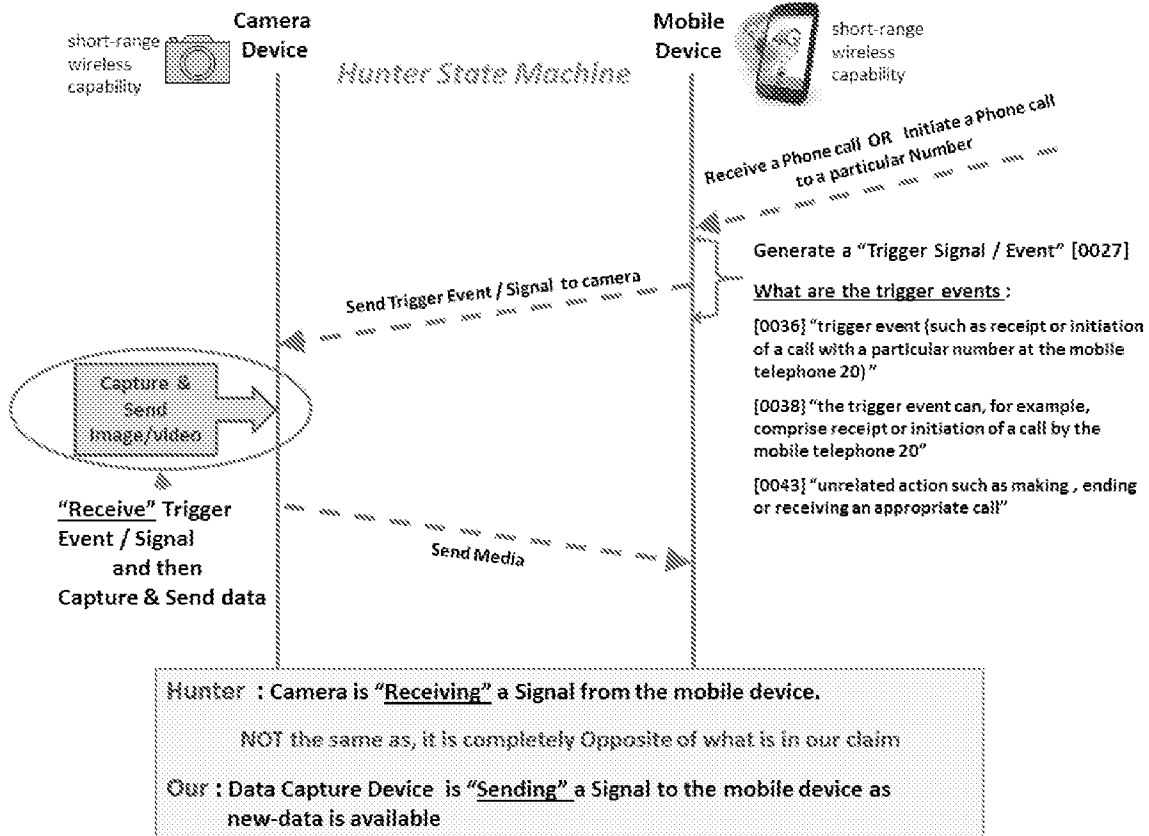
The sequence of events in Hunter is as follows:

- (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.

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.

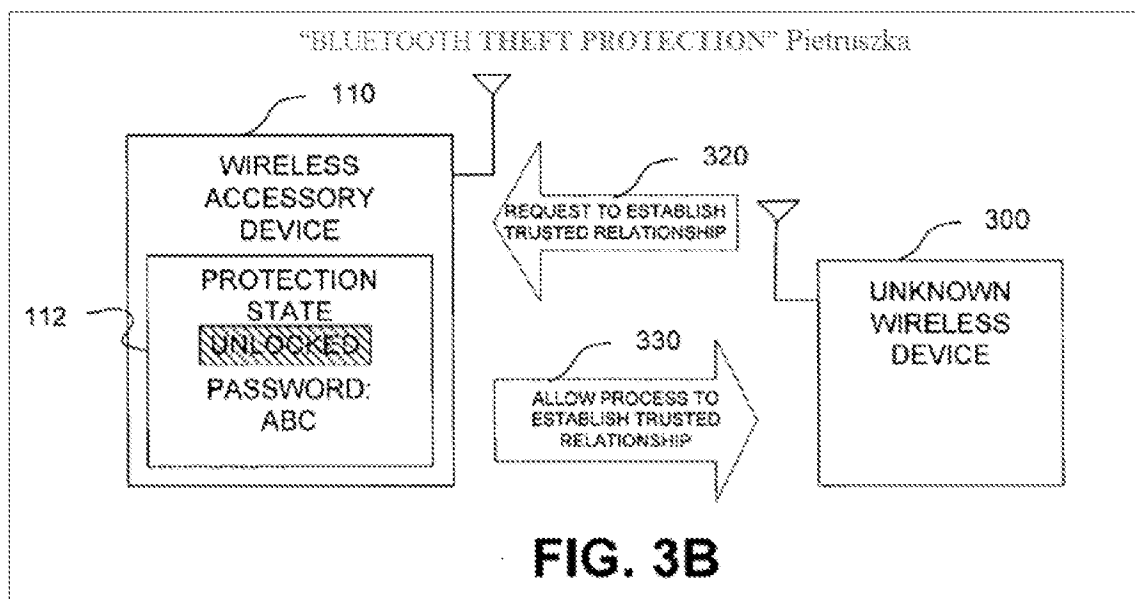
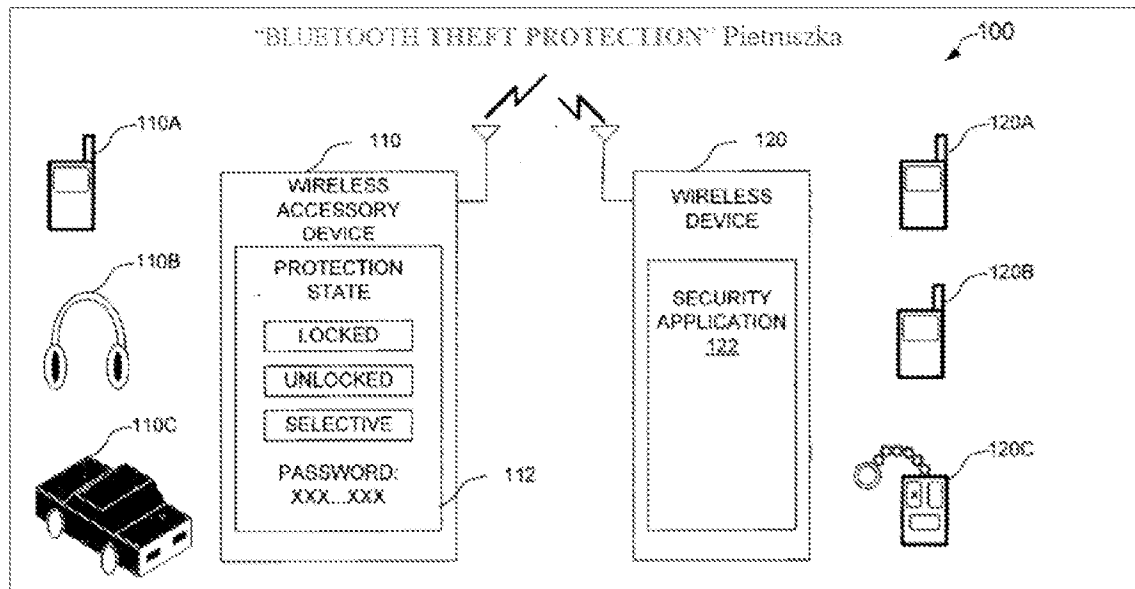
Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where a data capture device acquires new-data after a short-range paired wireless connection is established with a 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.



Argument #8:

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



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.

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:

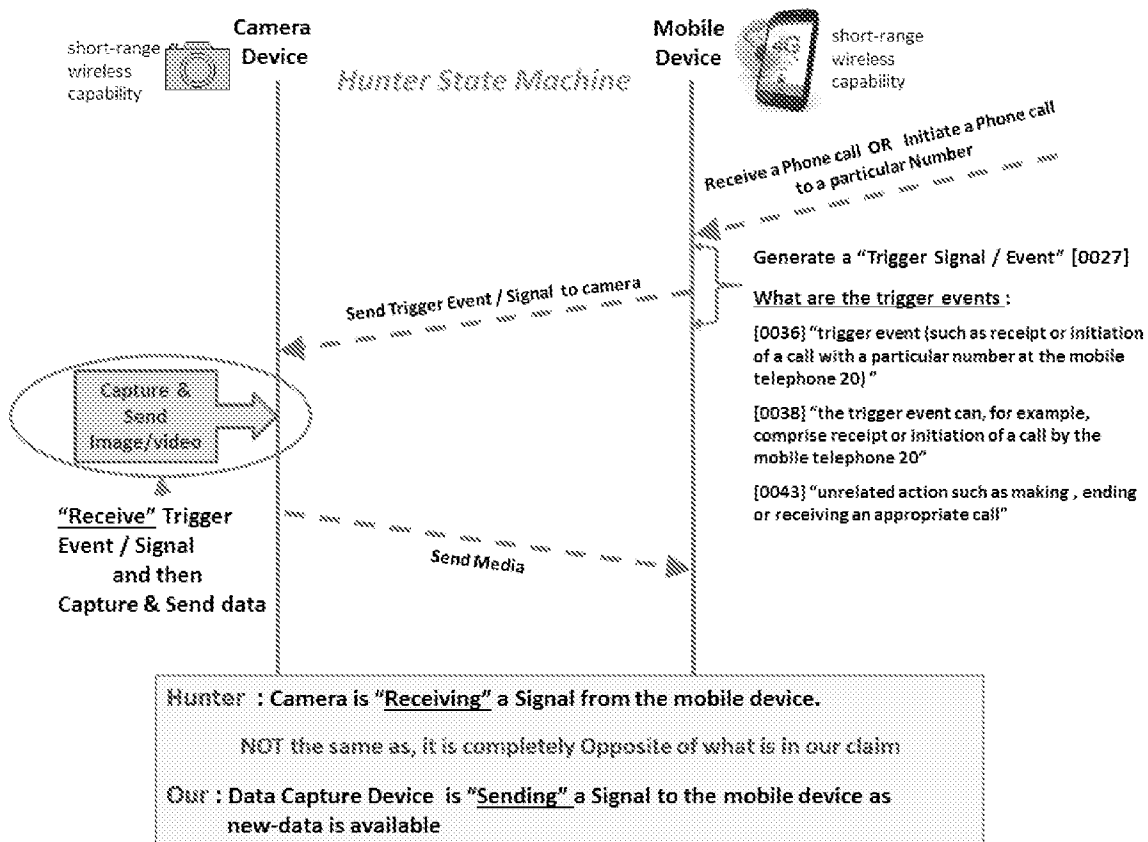
Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range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

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]:

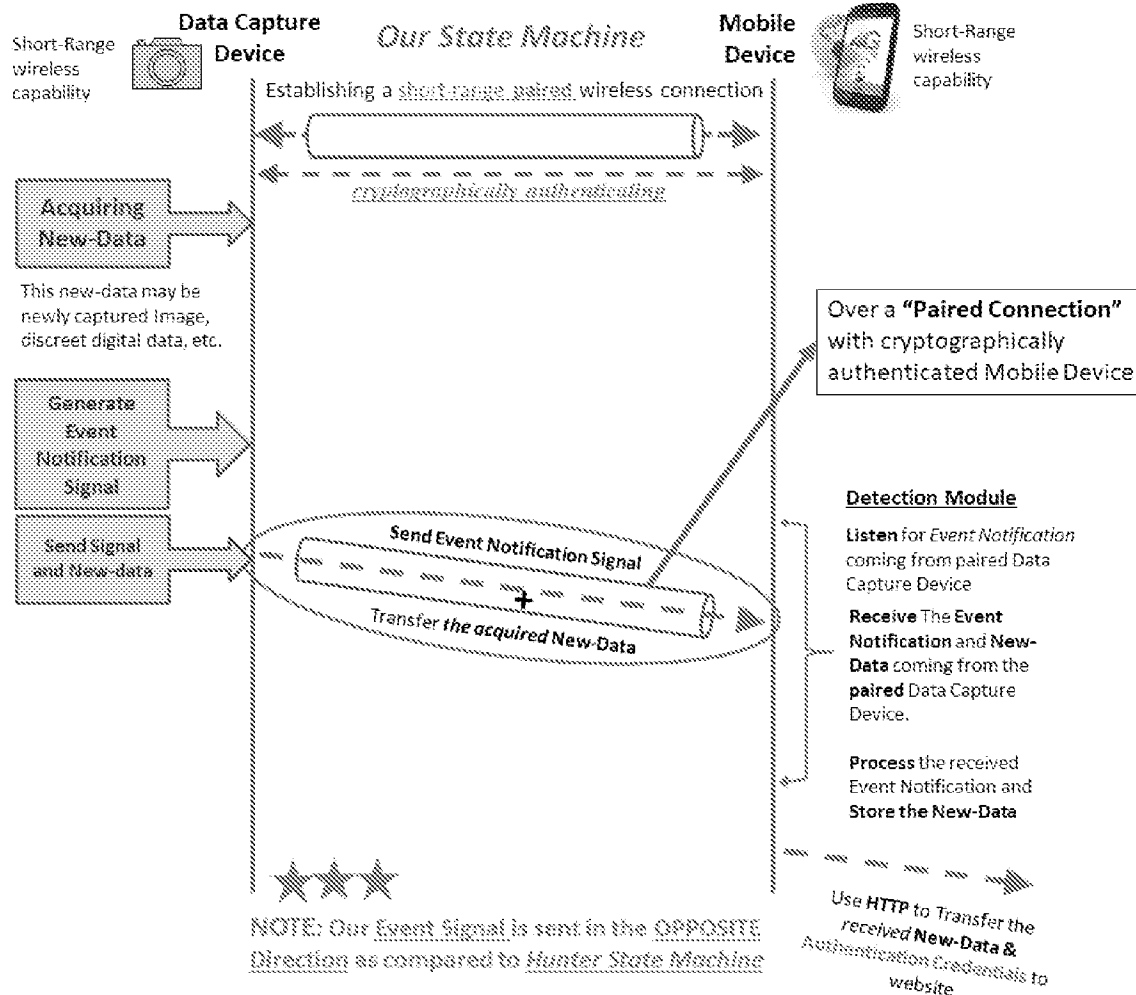


Firstly, in Hunter, there is NO cryptographic authentication of the mobile device by the data capture device before the signal is sent or the data is sent. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be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



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

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

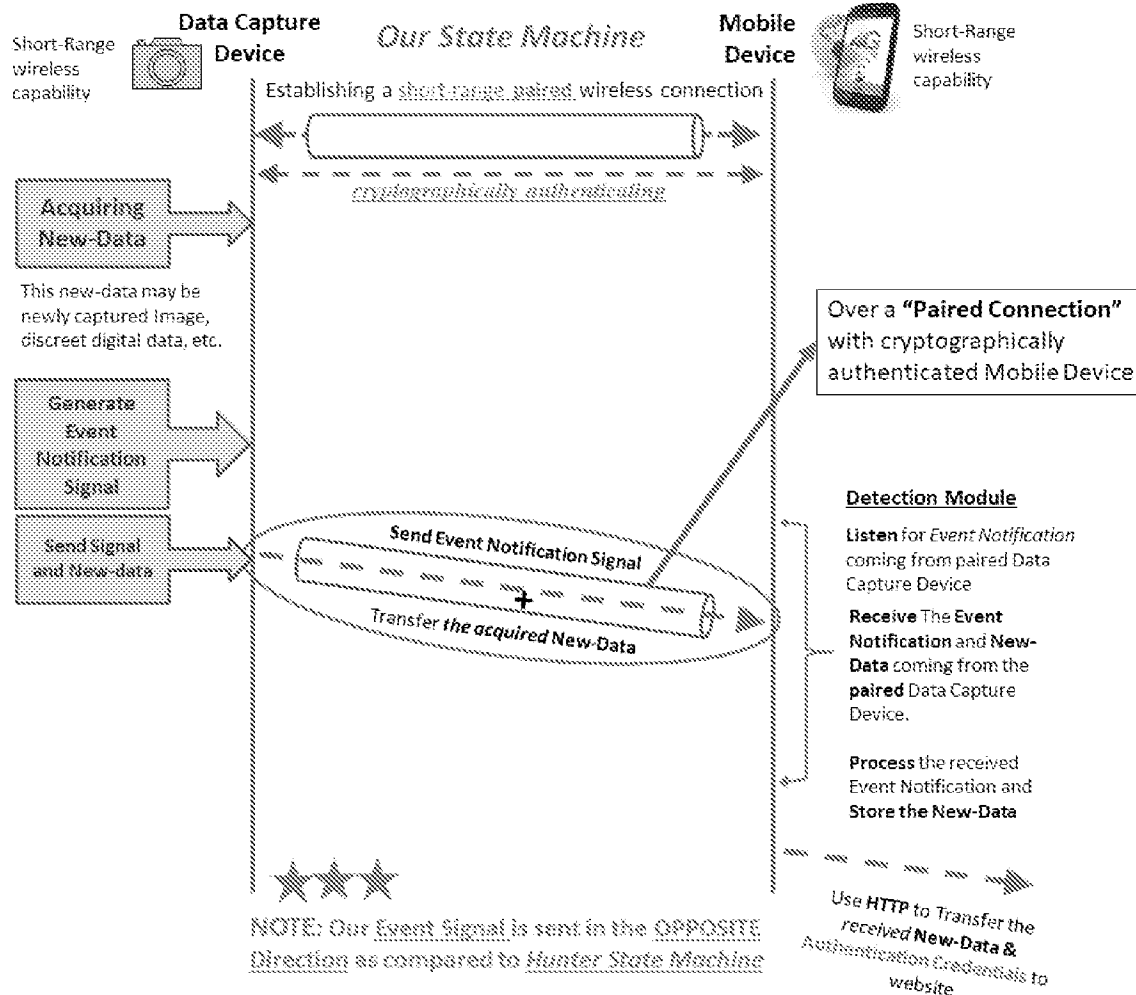
camera. Furthermore, in Hunter, the camera acquires the new-data only after it receives the trigger event or signal from the mobile device. In contrast, in applicant's disclosure, the polling request from the mobile phone to the camera is for detecting already acquired new data.

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



Comparison Table

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

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.

Date: September 01, 2021

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

Respectfully submitted,

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



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	EXAMINER	
ASHOK TANKHA 36 GREENLEIGH DRIVE SEWELL, NJ 08080			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

<i>Applicant-Initiated Interview Summary</i>	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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re. application of:

Gurvinder Singh

Application No.: 16/532,507

Filed: 08/06/2019

Applicant: Cellspinsoft Inc.

Title: Automatic Multimedia Upload

For Publishing Data And Multimedia Content

Examiner: Nooristany, Sulaiman

Art Unit: 2415

Atty. Docket no.: CellSpin_04Con17_US

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-

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:

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;

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;

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;

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

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.

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:*

<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*

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*

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.

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”.

- (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”.

(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 $\neq$ Sending

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

 **rec·og·nize**
/ˈrɛk.əɡ.naɪz/
verb
gerund or present participle: recognizing

1. identify (someone or something) from having encountered them before; know again.
"I recognized her when her wig fell off"
2. acknowledge the existence, validity, or legality of.
"the defense is recognized in Mexican law"

Similar: acknowledge accept admit concede allow grant confess ▼

Definitions from Oxford Languages

(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:

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:

provide a touch based graphical user interface for the received new-data (Hunter: [0025], Pietruszka [0099])	
Hunter [0025] In any event, once a data link has been established, the image capture device may be arranged to periodically transmit a frame of image data to the mobile telephone to be transmitted, stored or discarded, according to whether or not the mobile telephone user actually wishes to transmit image data at that time. In a preferred embodiment, the mobile telephone may comprise a selection switch which, when actuated, causes image data to be selectively stored or transmitted across the telephone network. Thus, if the selection switch is not actuated, no image data is stored or transmitted, and image data (if any) sent from the image capture device to the mobile telephone is discarded. Alternatively or additionally, there may be a means to activate storage or transmission of images to a mobile telephone as a result of an operation of the camera, such as a touch or voice command.	Pietruszka [0099] 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 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.
➤ In Hunter [0025] the touch interface and operation is on the Camera device and for the image taken on/by the camera. ➤ In our claims the touch interface is on the Mobile device and is for the image received from the camera. ➤ Two completely different devices and for two completely different reasons.	➤ In Pietruszka [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. ➤ In our claims the touch based user interface is for the “received new-data”

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”

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.

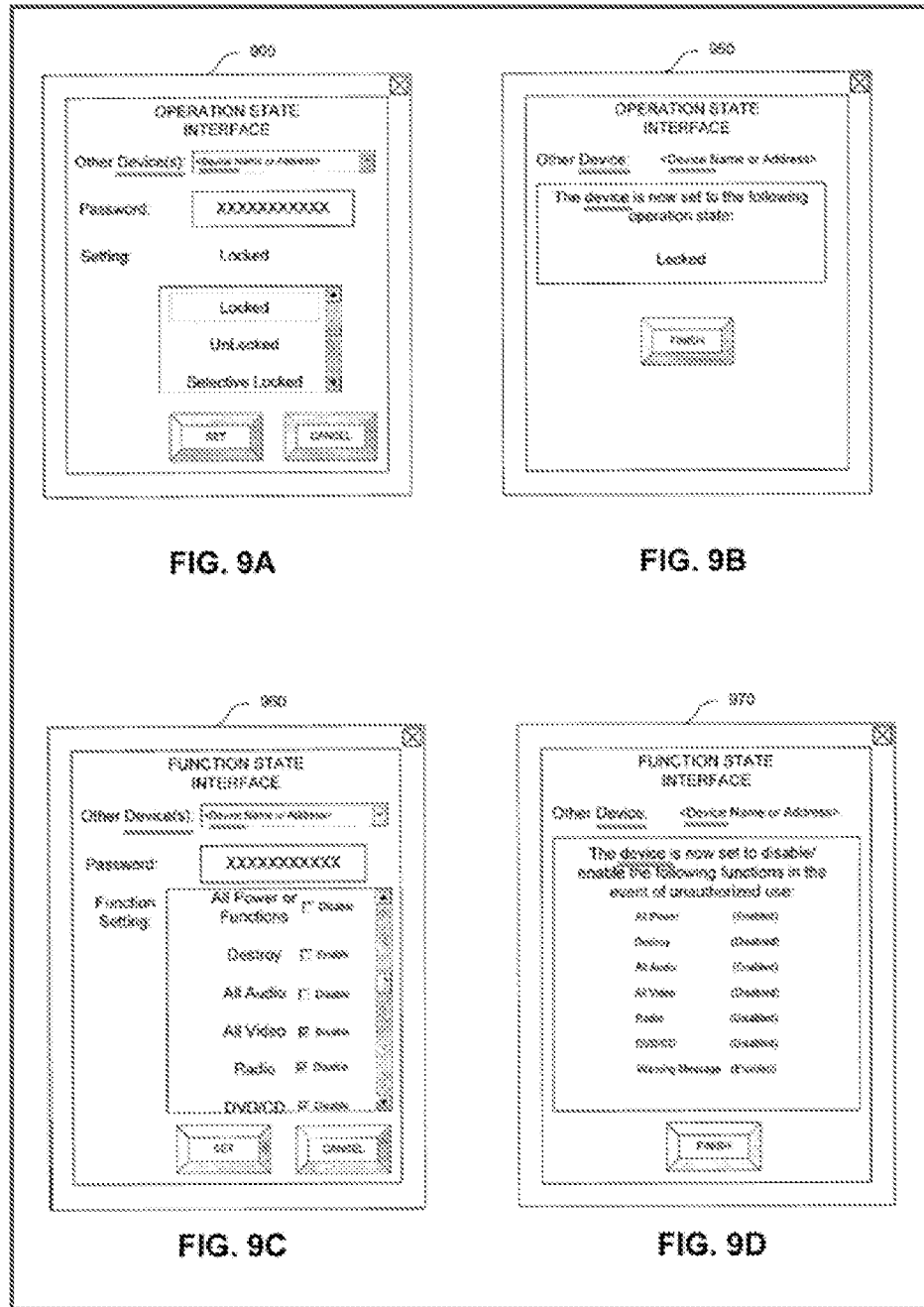
Therefore, applicant submits that “*Cryptographic authentication of a wireless device*” in Pietruszka is not same as “*Website user authentication credentials*” as recited in applicant’s claim 1.

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.



- 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

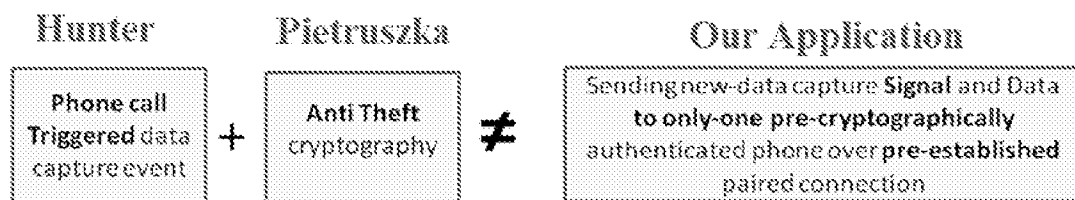
Cryptographic authentication of a wireless device

≠

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,

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.

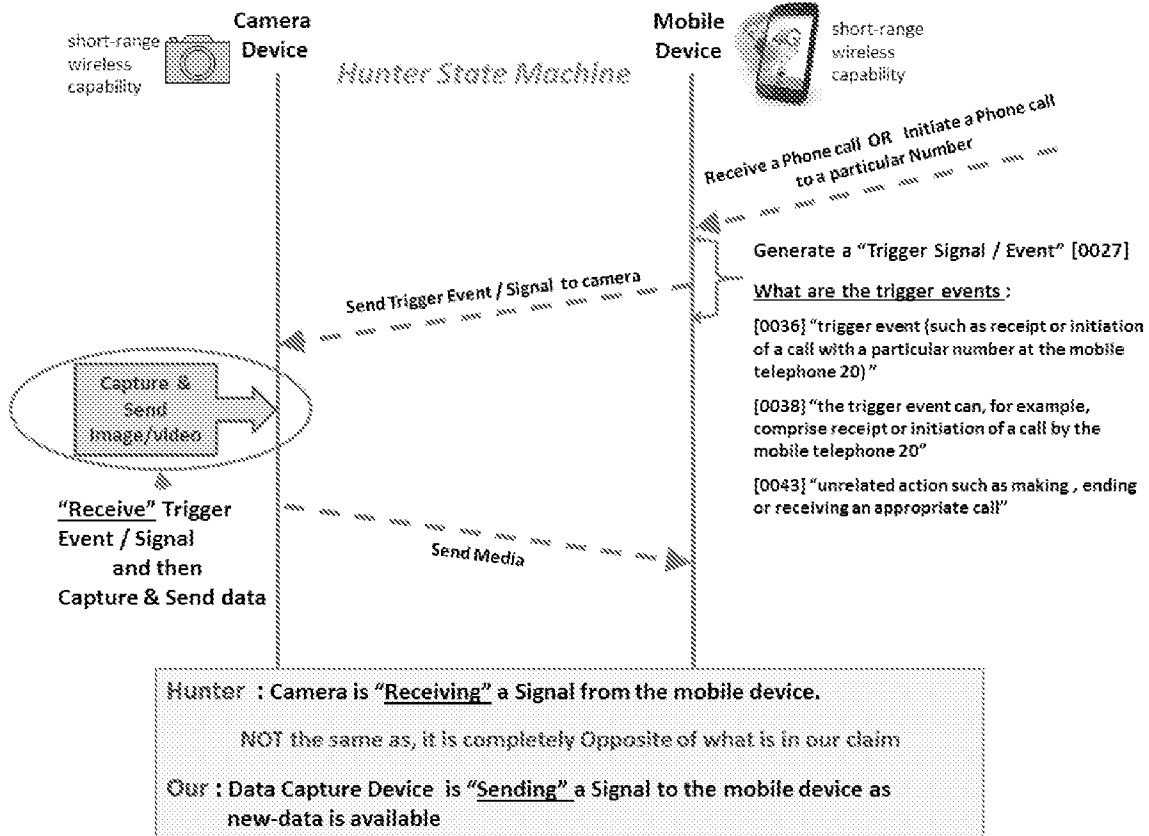
The sequence of events in Hunter is as follows:

- (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.

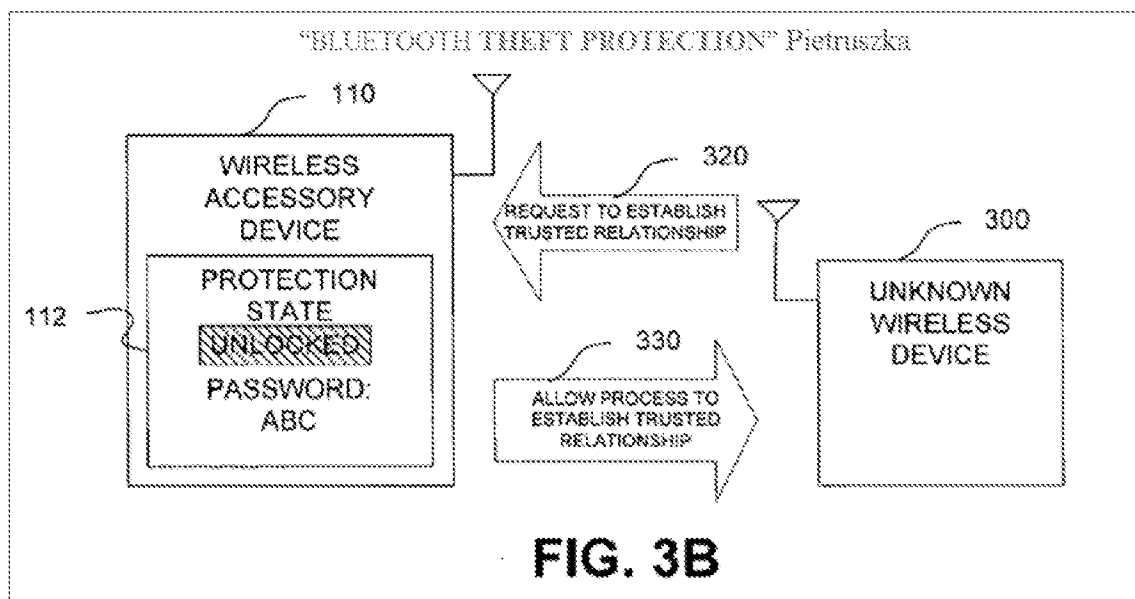
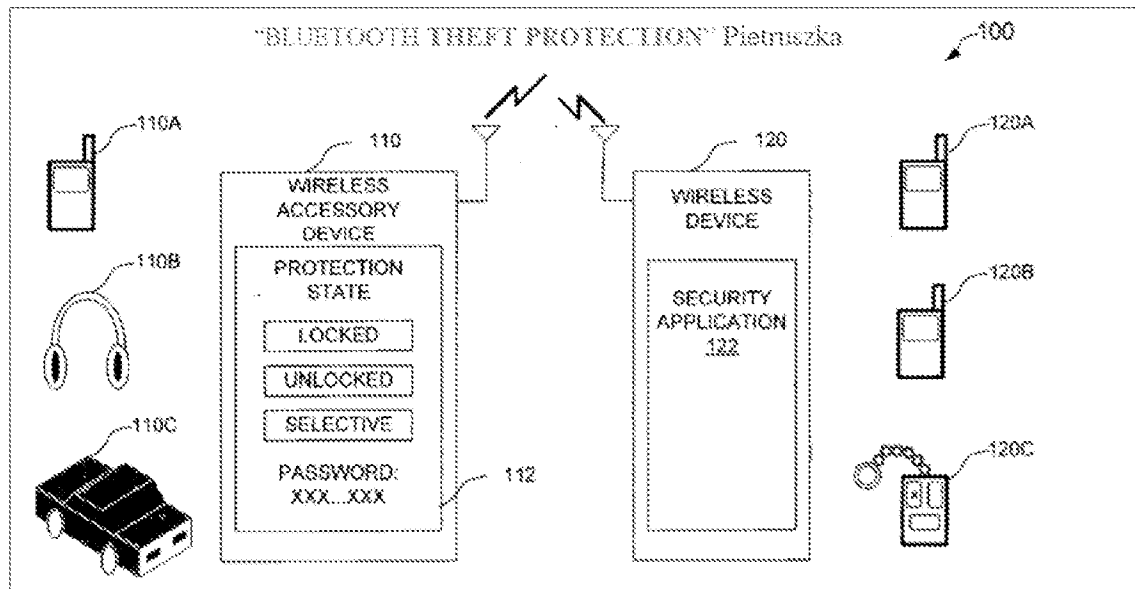
Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where a data capture device acquires new-data after a short-range paired wireless connection is established with a 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.



Argument #7:

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



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.

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:

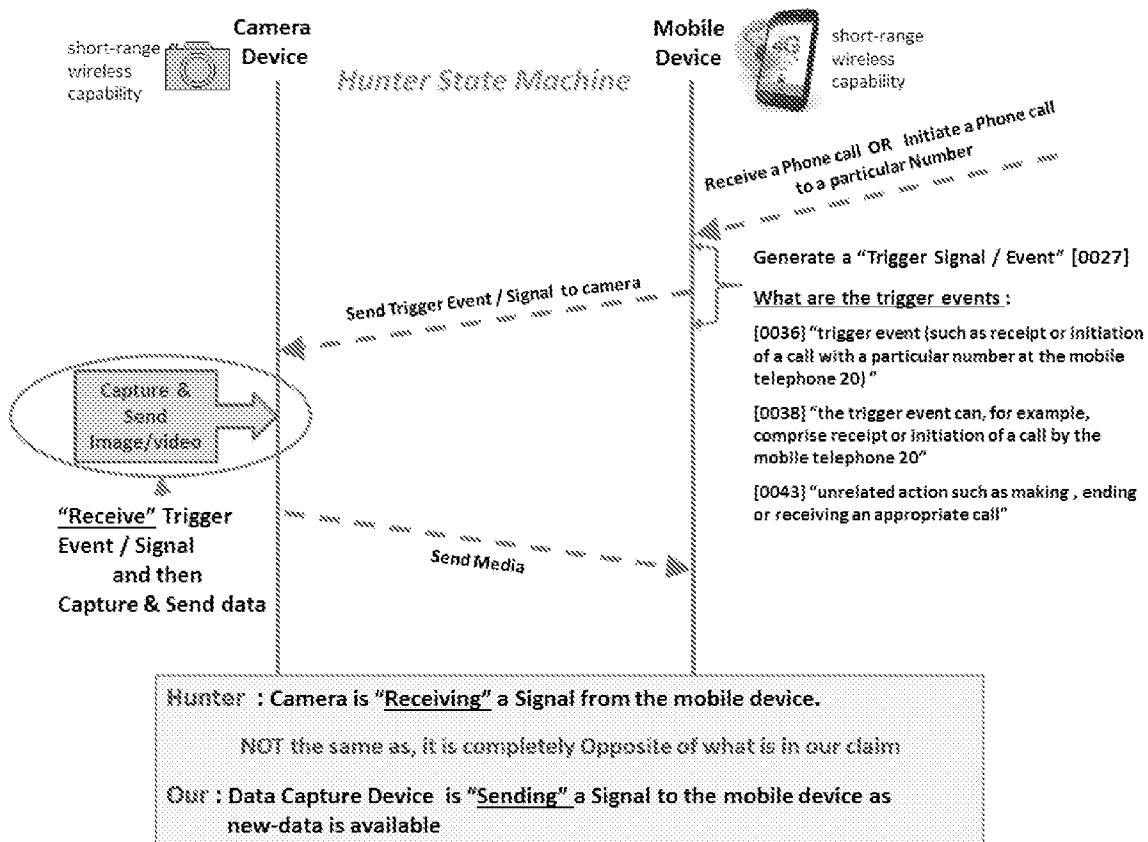
Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range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

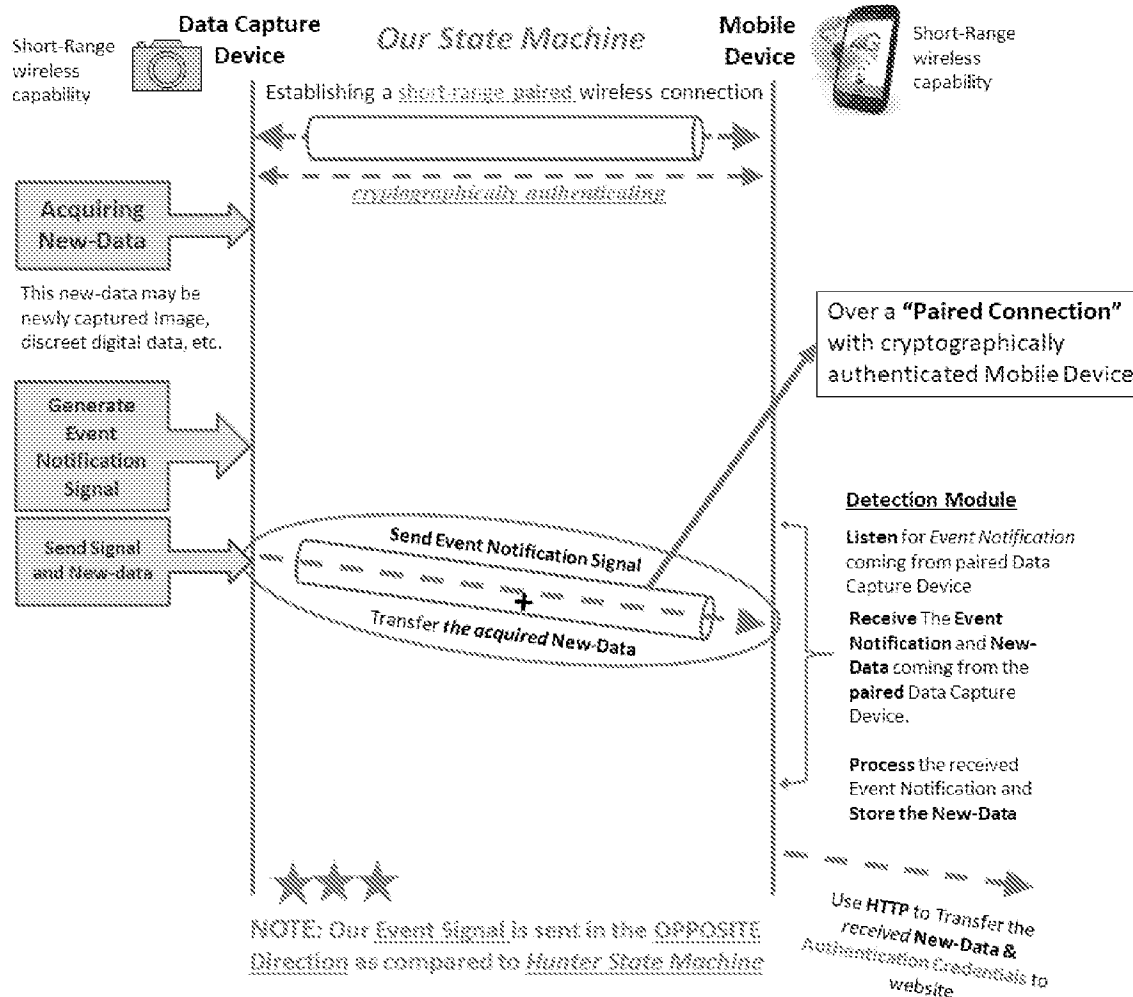


Firstly, in Hunter, there is NO cryptographic authentication of the mobile device by the data capture device before the signal is sent or the data is sent. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be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



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 #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.

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:

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.**

Summary

Comparison Table

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

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

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.”

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

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

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

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.

Date: July 21, 2021

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

Respectfully submitted,

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re. application of:

Gurvinder Singh

Application No.: 16/532,507

Filed: 08/06/2019

Applicant: Cellspinsoft Inc.

Title: Automatic Multimedia Upload

For Publishing Data And Multimedia Content

Examiner: Nooristany, Sulaiman

Art Unit: 2415

Atty. Docket no.: CellSpin_04Con17_US

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 February 09, 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-

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:

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;

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;

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;

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;

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

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.

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

Double Patenting

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

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 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 1-9, 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.

Amendments to the claims

Claims 7 and 14 are currently amended; claims 1-6 and 8-13 remain as previously presented. Applicant respectfully submits that the amendments to the claims do not add any new subject matter.

Support for claim amendments

Support for the amendment: “*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.”*
- (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 [0034] of Exhibit B, which states: “*The publishing service 204 comprises a database 204a, the front end service 204b, a back end service 204c, and a user authentication module 204g. The database 204a of the publishing service 204 comprises user profiles, user preferences.”*
- (f) Paragraph [0037] of Exhibit B, which states: “*The back end service 204c then transfers the multimedia object to the front end service 204b. The front end service 204b associates the multimedia object with the user preferences and*

publishes the multimedia object on one or more publication virtual spaces 205 via the network 203”.

- (g) 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.*”
- (h) 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.*”
- (i) 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 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 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.

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”.
- (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”.
- (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 1-9, 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.**”

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 $\neq$ Sending

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



rec·og·nize

/ˈrɛkəɡ.nɪz/

verb

gerund or present participle: recognizing

1. identify (someone or something) from having encountered them before; know again.
"I recognized her when her wig fell off"
2. acknowledge the existence, validity, or legality of.
"the defense is recognized in Mexican law"

Similar: acknowledge accept admit concede allow grant confess

Definitions from Oxford Languages

(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:

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:

provide a touch based graphical user interface for the received new-data (Hunter: [0025], Pietruszka [0099])	
Hunter [0025] In any event, once a data link has been established, the image capture device may be arranged to periodically transmit a frame of image data to the mobile telephone to be transmitted, stored or discarded, according to whether or not the mobile telephone user actually wishes to transmit image data at that time. In a preferred embodiment, the mobile telephone may comprise a selection switch which, when actuated, causes image data to be selectively stored or transmitted across the telephone network. Thus, if the selection switch is not actuated, no image data is stored or transmitted, and image data (if any) sent from the image capture device to the mobile telephone is discarded. Alternatively or additionally, there may be a means to activate storage or transmission of images to a mobile telephone as a result of an operation of the camera, such as a touch or voice command.	Pietruszka [0099] 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 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.
➤ In Hunter [0025] the touch interface and operation is on the Camera device and for the image taken on/by the camera. ➤ In our claims the touch interface is on the Mobile device and is for the image received from the camera. ➤ Two completely different devices and for two completely different reasons.	➤ In Pietruszka [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. ➤ In our claims the touch based user interface is for the “received new-data”

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”

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.

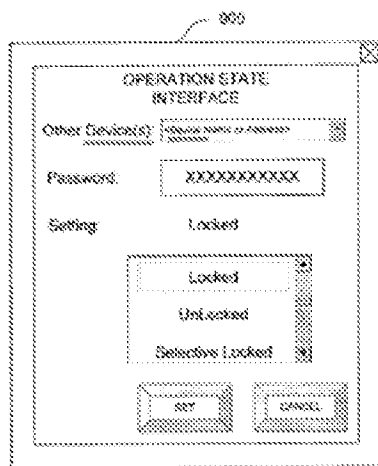


FIG. 9A

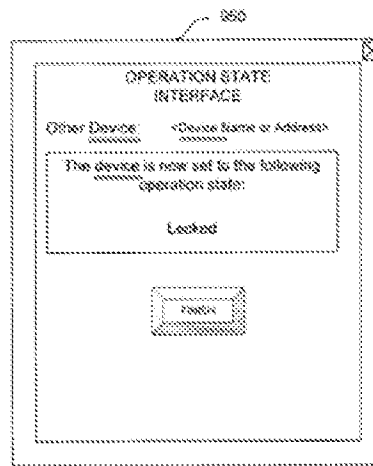


FIG. 9B

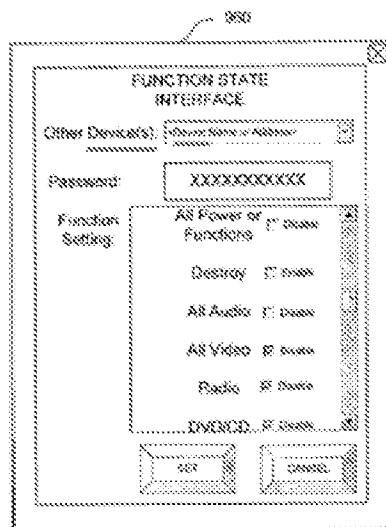


FIG. 9C

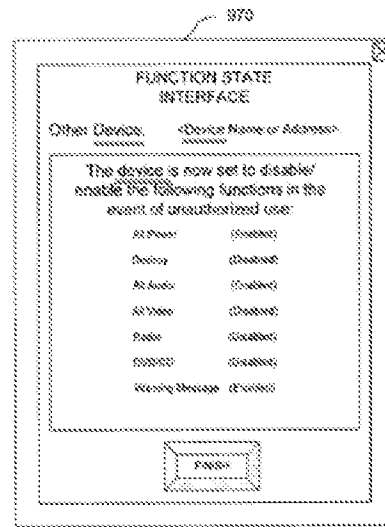


FIG. 9D

- 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

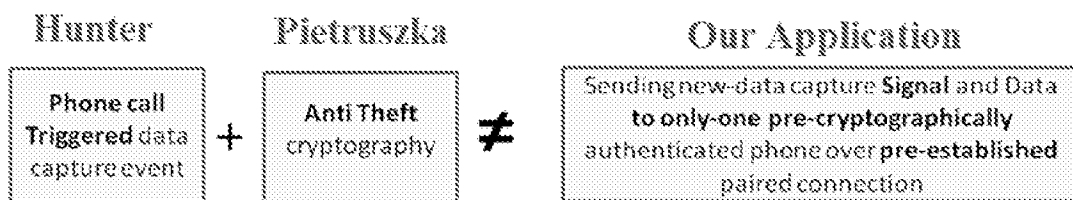
Cryptographic authentication of a wireless device

≠

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,

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.

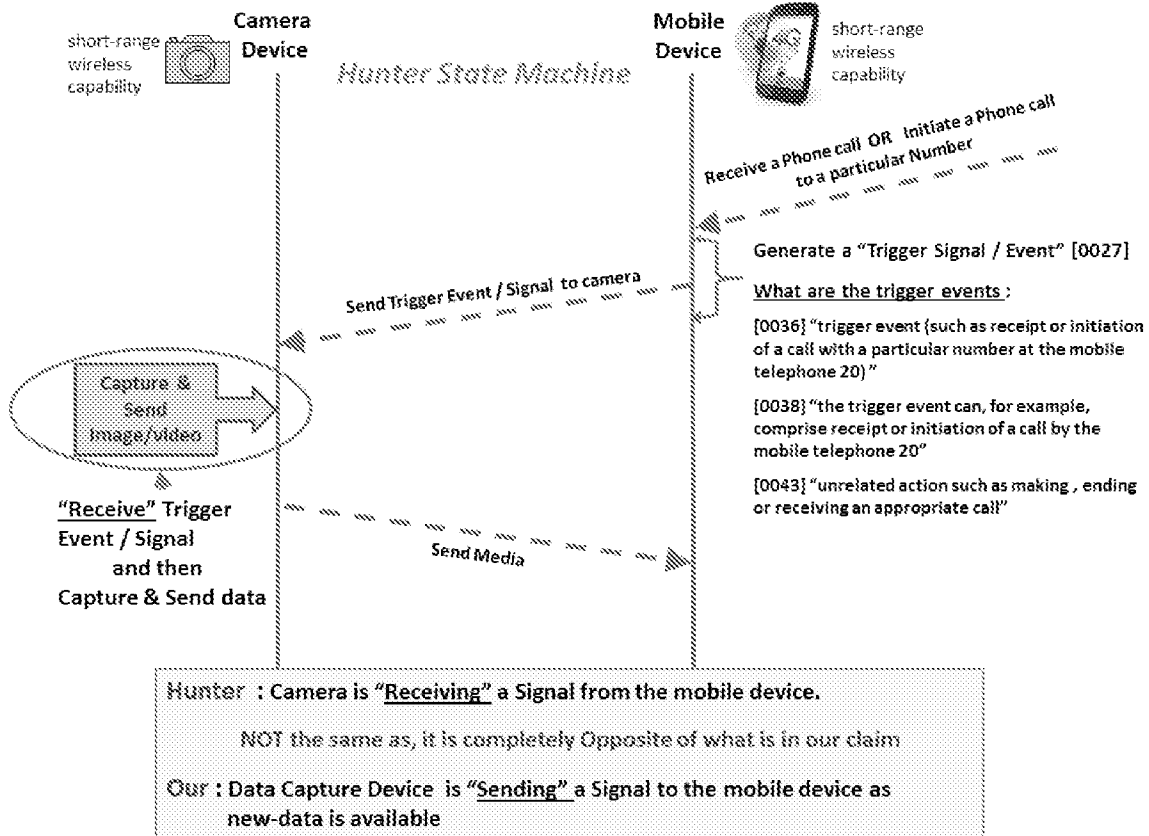
The sequence of events in Hunter is as follows:

- (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.

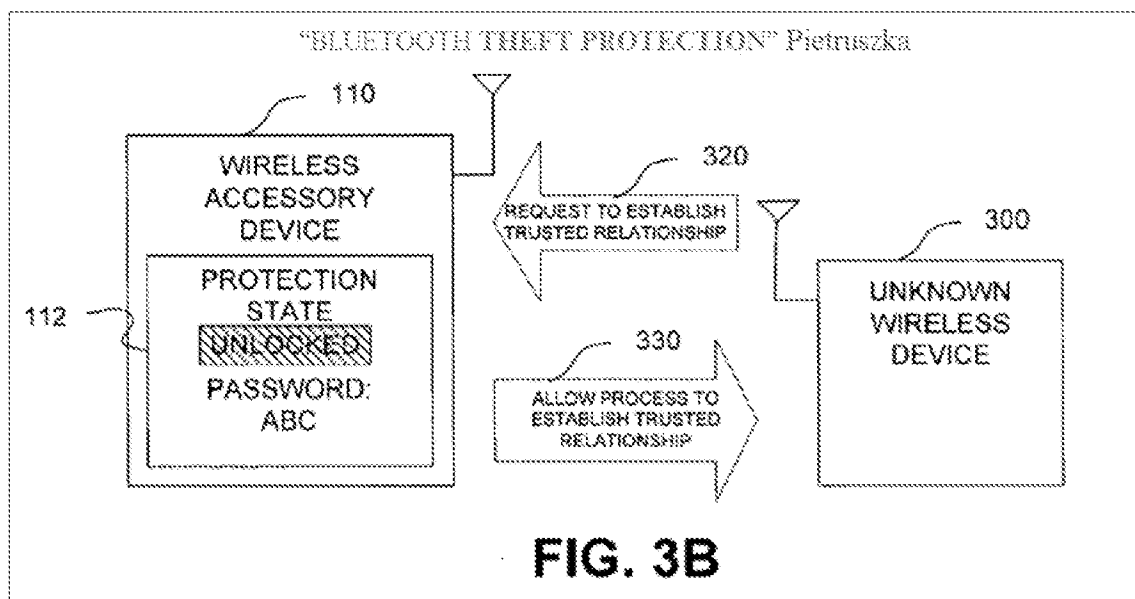
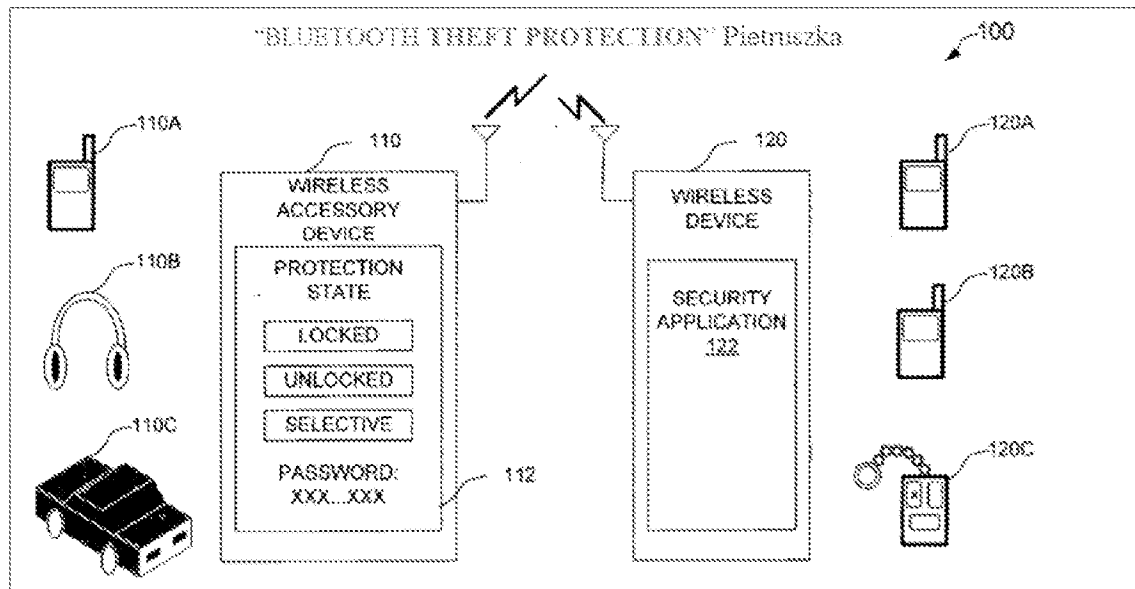
Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where a data capture device acquires new-data after a short-range paired wireless connection is established with a 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.



Argument #7:

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



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.

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:

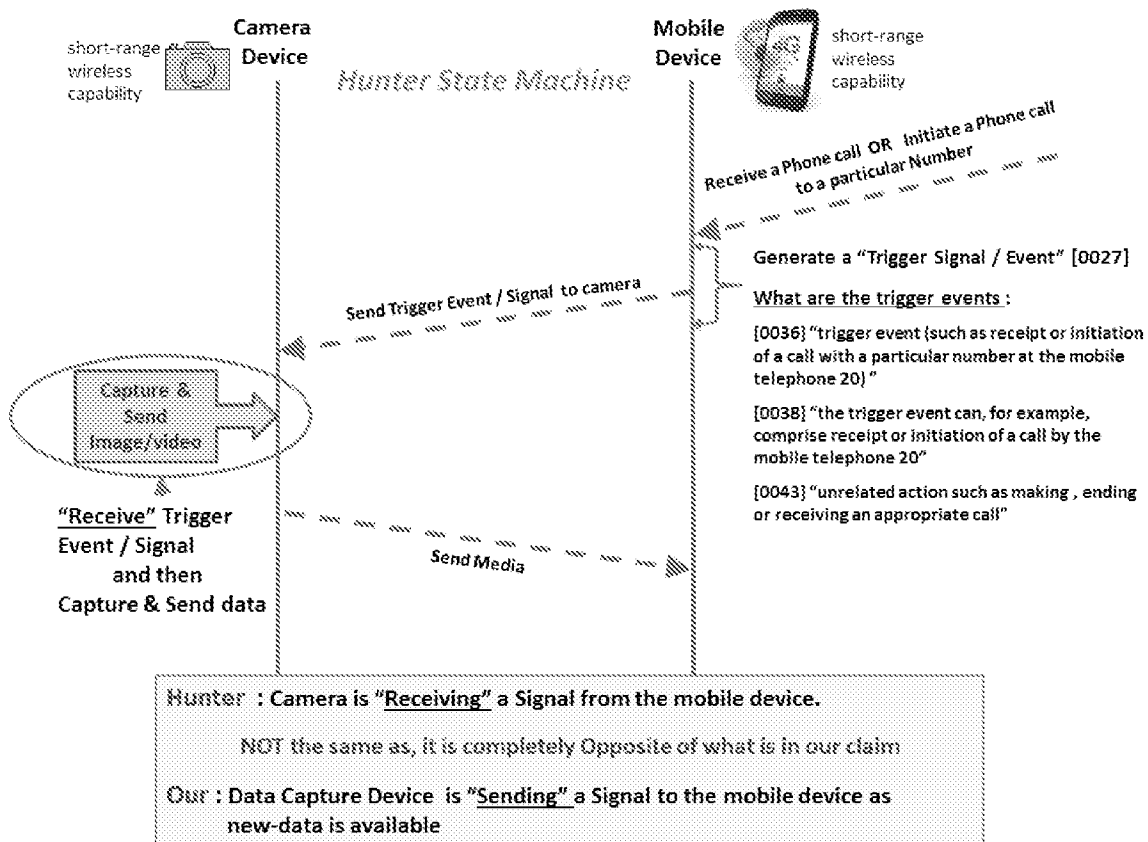
Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range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

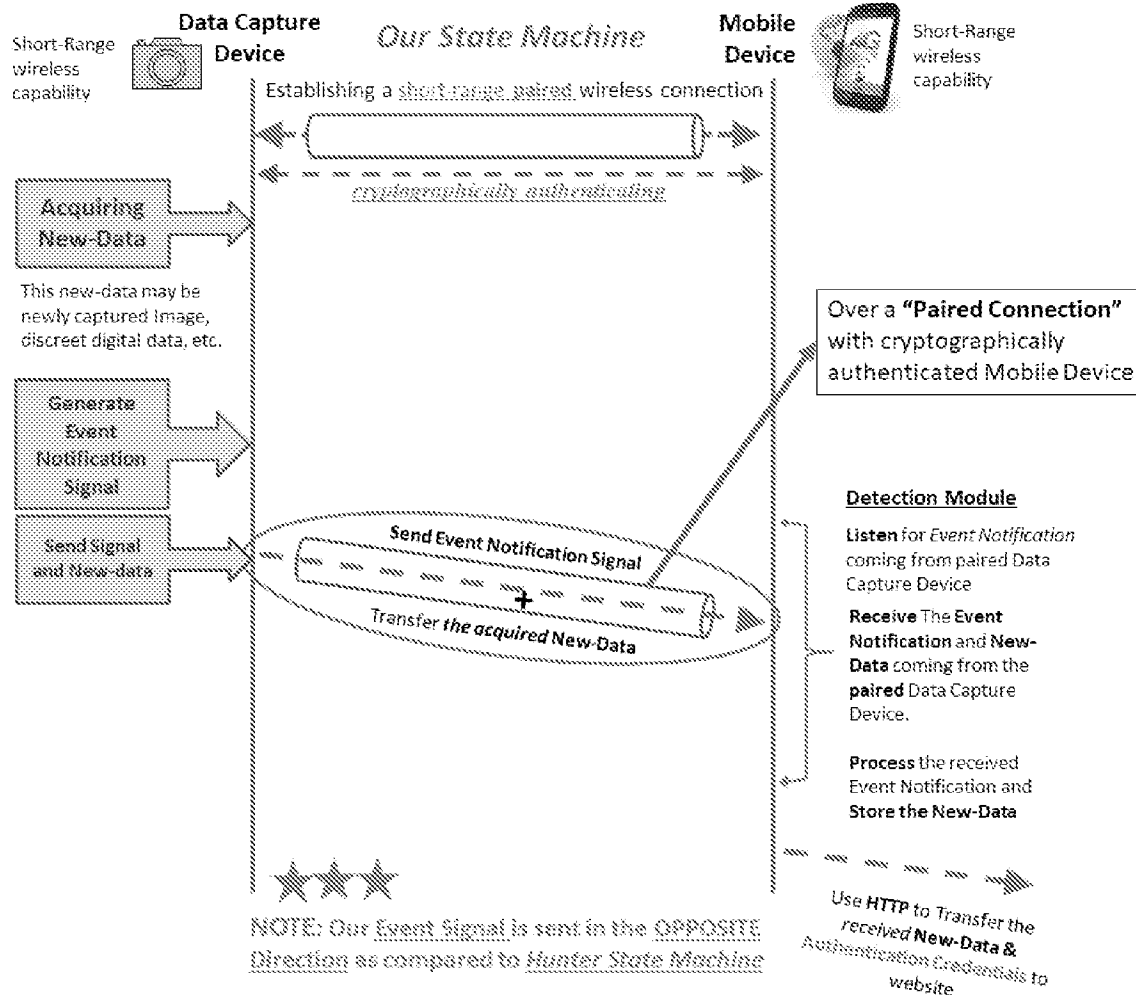


Firstly, in Hunter, there is NO cryptographic authentication of the mobile device by the data capture device before the signal is sent or the data is sent. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be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



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 #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.

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:

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

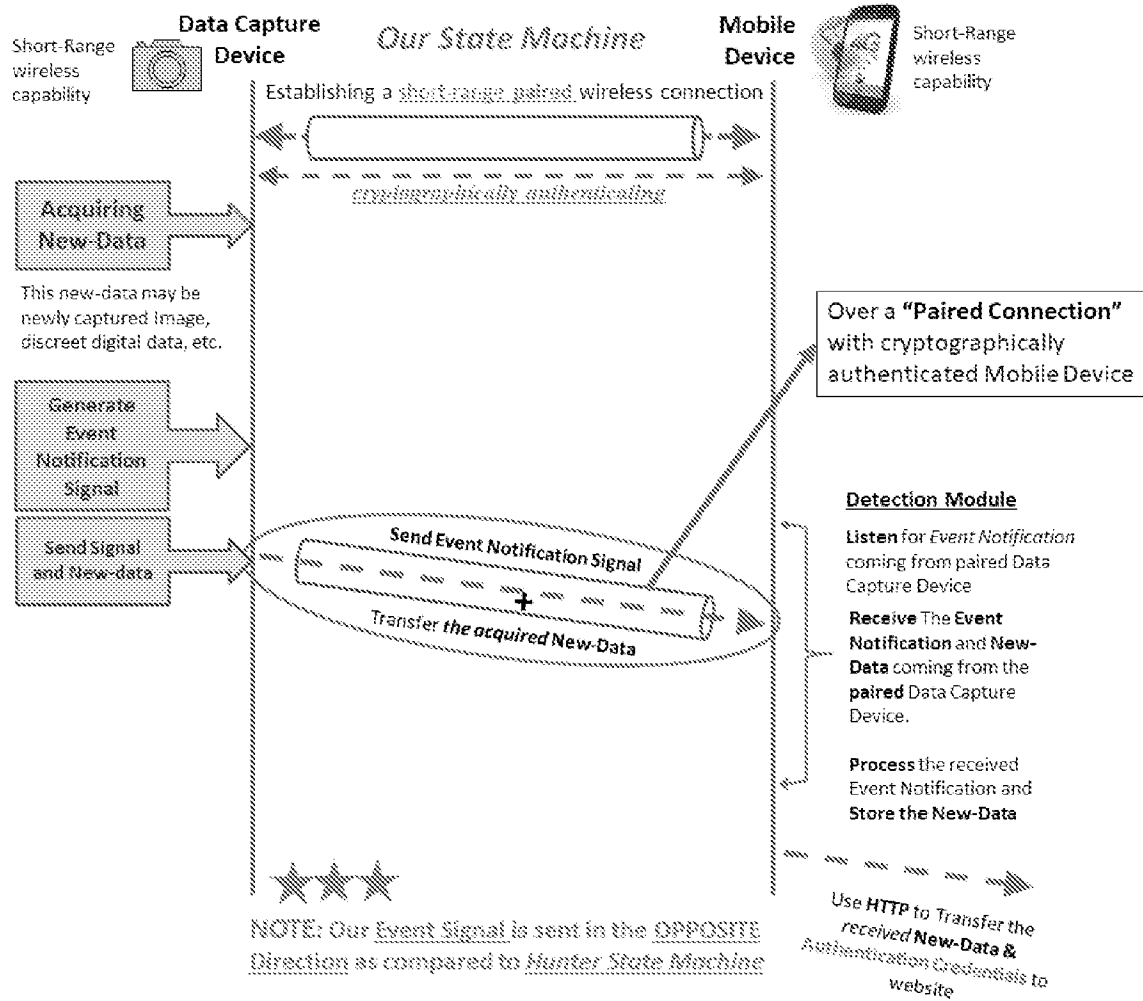
As illustrated before, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate the trigger event or signal to be sent to the camera. Furthermore, in Hunter, the camera acquires the new-data only after it receives the trigger event or signal from the 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.

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 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;”

Summary

Applicant's state machine



Comparison Table

Claim Feature	Hunter	Pietruszka	Applicant Cellspin
1 Pairing for new-data transfer.	NO mention of pairing. Pairing is NOT established. <u>Teaching away</u> from establishing permanent connection.	NO Invention is about <u>selecting or preventing, and controlling</u> pairing between devices. NOT for new-data transfer	YES <u>Pairing</u> is established to transfer the acquired new-data.
2 Cryptographically authenticate the identity of Mobile Device	NO	YES <u>Only if wireless communication device is unlocked for pairing.</u>	YES The Mobile device is cryptographically authenticated by the data capture device <u>NOT based on pre-selection of activation or deactivation of pairing.</u>
3 Sending new data capture Event Notification Signal	NO <u>Trigger Event Signal is sent from the mobile device to the camera device, which is opposite to applicant's invention.</u>	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 <u>data capture device to cellular phone after acquiring new-data.</u>
4 Send data to the mobile device over a <u>pre-established paired</u> connection	NO	NO <u>There is no data to transfer.</u>	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 <u>After pairing is established</u>
6 Data transfer between two devices happens <u>over what type of wireless link?</u>	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 claim 1, 4, 8 and 12.

Therefore, claims 4, 8 and 12 are also non-obvious over Hunter, in view of Pietruszka. Claims 2-3 are dependent on claim 1; claims 5-7 are dependent on claim 4; claim 11 is dependent on claim 8; claims 13-14 are dependent on claim 12. Applicant therefore respectfully submits that dependent claims 2-3, 5-7, 9 and 13-14 are also non-obvious over Hunter, in view of Pietruszka.

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.

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.

Date: May 05, 2021

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

Respectfully submitted,

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



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	EXAMINER	
ASHOK TANKHA 36 GREENLEIGH DRIVE SEWELL, NJ 08080			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

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 37 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).

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.

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.

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 negated by the manner in which the invention was made.

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**);

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:

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]**);

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.

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.

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

Art Unit: 2415

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:

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:

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

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

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