

Doc code: RCEX

Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (02-18)

Approved for use through 11/30/2020. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

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

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.

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

SUBMISSION REQUIRED UNDER 37 CFR 1.114

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

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

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

☐ Other _____

☒ Enclosed

☒ Amendment/Reply

☐ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

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

☐ Other _____

FEES

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

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature
Applicant Signature

Doc code: RCEX

Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (02-18)

Approved for use through 11/30/2020. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

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

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

Privacy Act Statement

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

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

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

Amendments to the claims

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

Amendments to the claims

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

a memory device;

a processor coupled to the memory device;

a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone, wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled data capture device cryptographically authenticating identity of the short-range wireless enabled cellular phone;

a data capture circuitry;

said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;

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

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 recognising occurrence of the trigger event, and communicating with the other of the camera and the communications device by a wireless link therebetween; transferring images between the camera and the communications device over the wireless link; and transferring said images from the communications device on to a data network through a data network interface.

Recognizing ≠ Sending

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



rec·og·nize
 /ˈrɪk.ə.ɡ.aɪz/

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 #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.

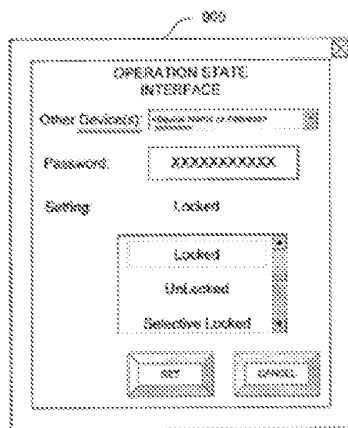


FIG. 9A

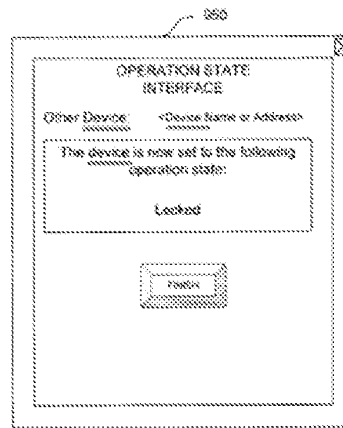


FIG. 9B

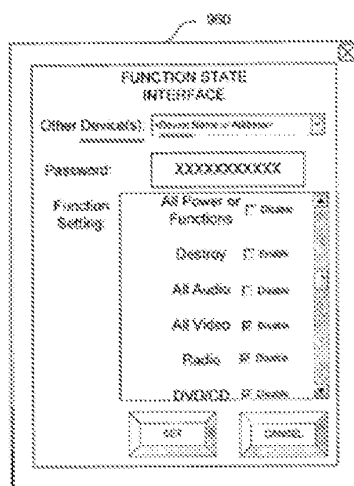


FIG. 9C

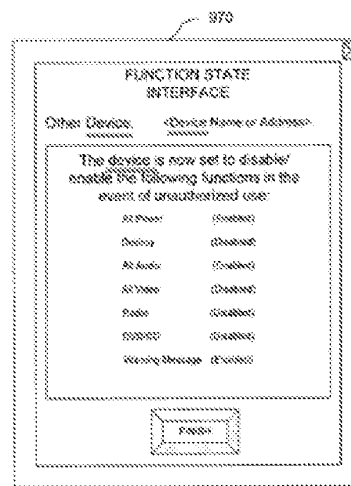


FIG. 9D

- 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

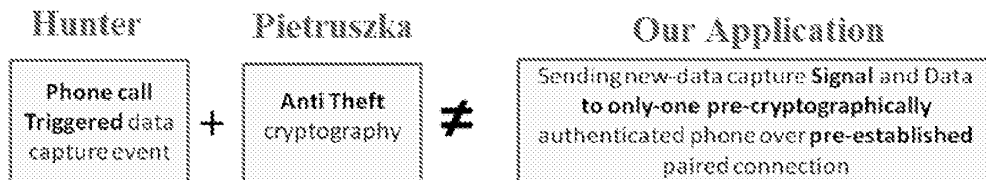
Cryptographic authentication of a wireless device

≠

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.

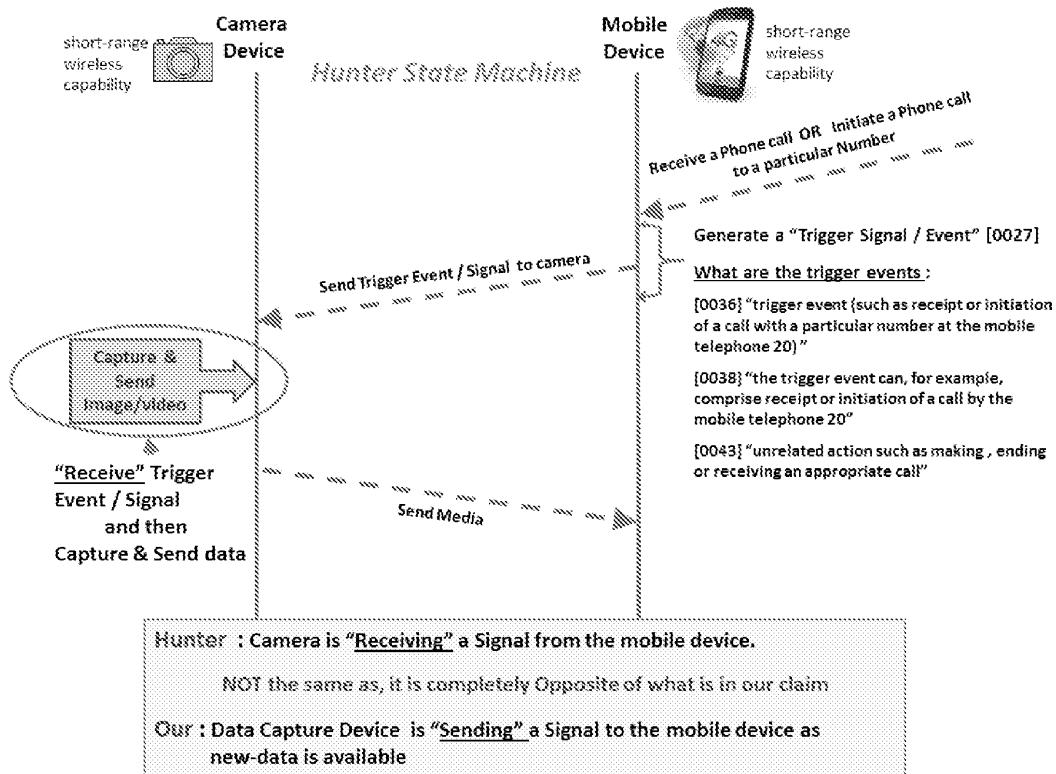
The sequence of events in Hunter is as follows:

- (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.

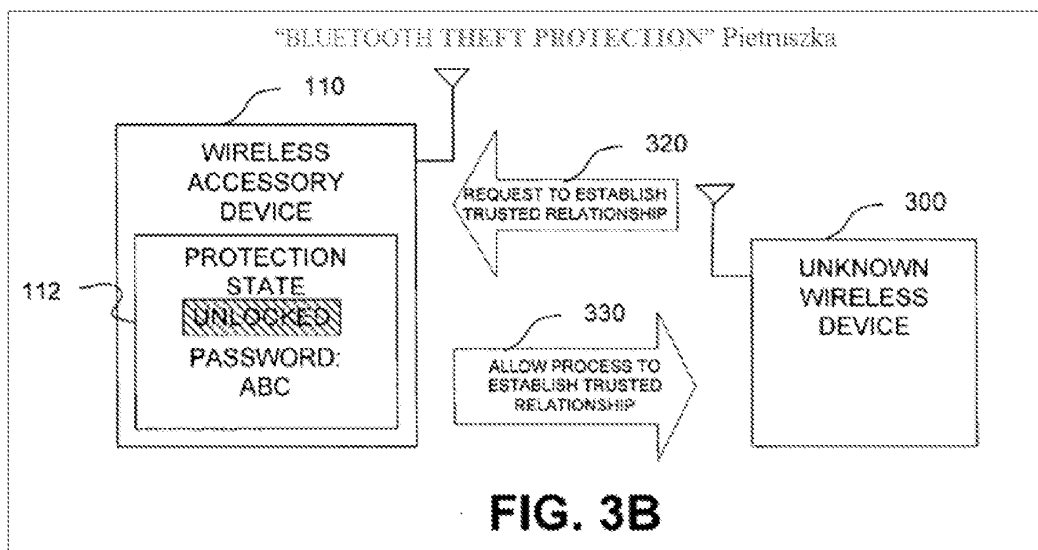
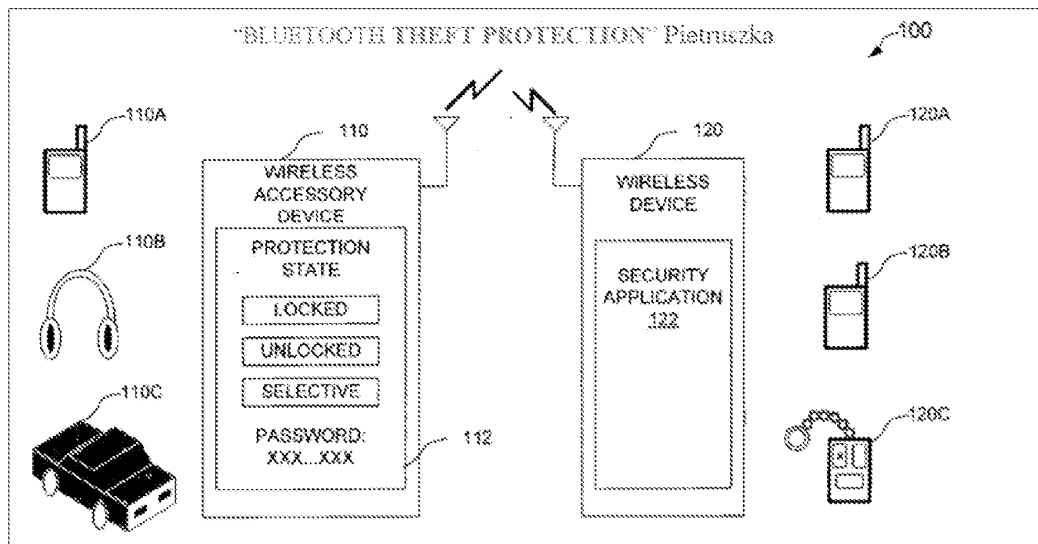
Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where a data capture device acquires new-data after a short-range paired wireless connection is established with a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

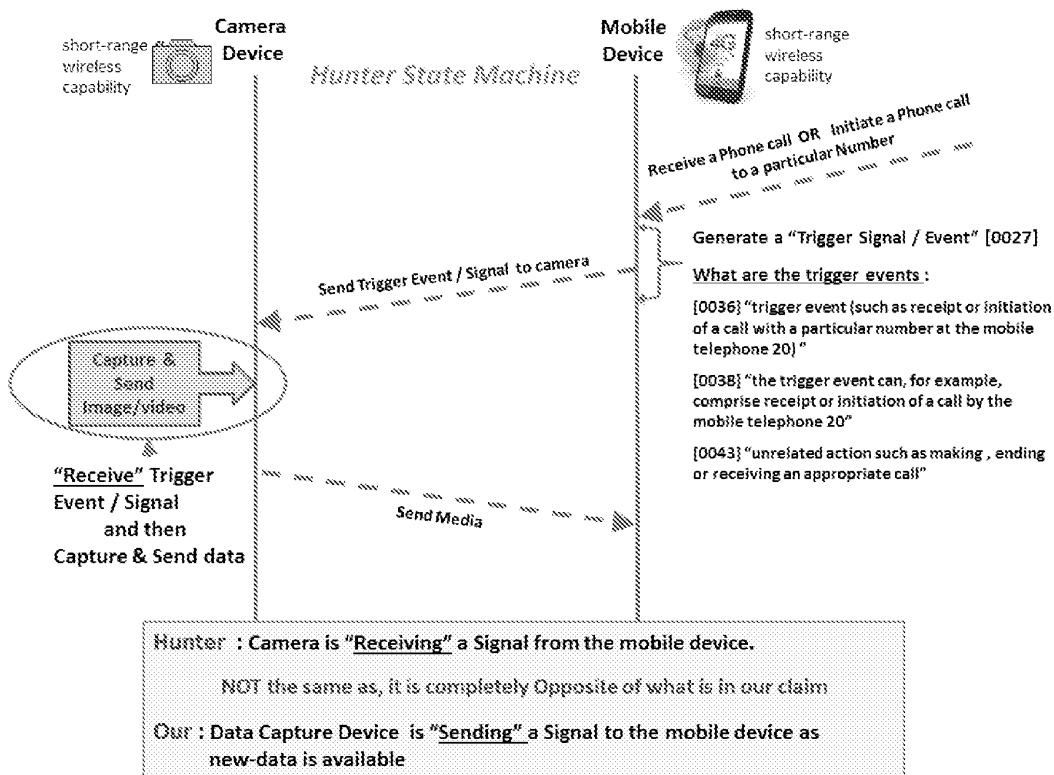
Sending an event notification and acquired new-data to a cryptographically authenticated short-range wireless enabled cellular phone over an established short-range paired wireless connection, where sending the event notification comprises sending a signal to the cryptographically authenticated short-range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

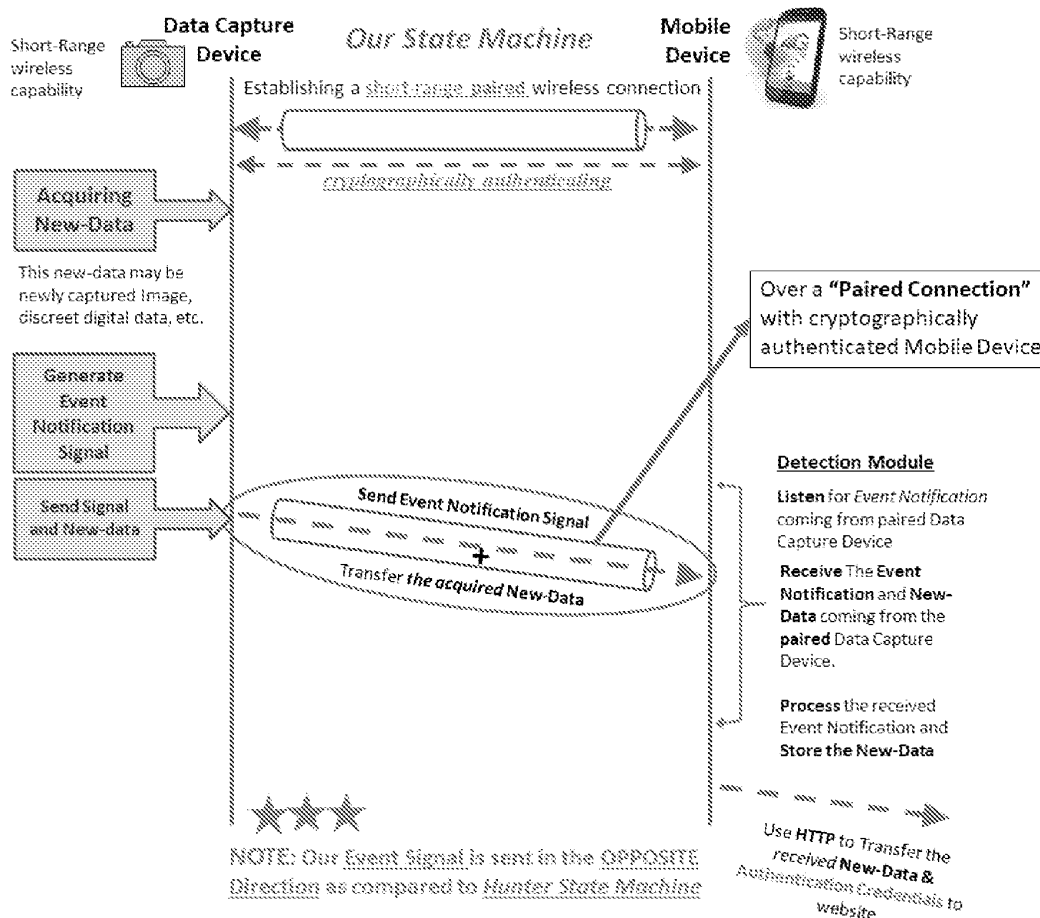


Firstly, in Hunter, there is NO cryptographic authentication of the mobile device by the data capture device before the signal is sent or the data is sent. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be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

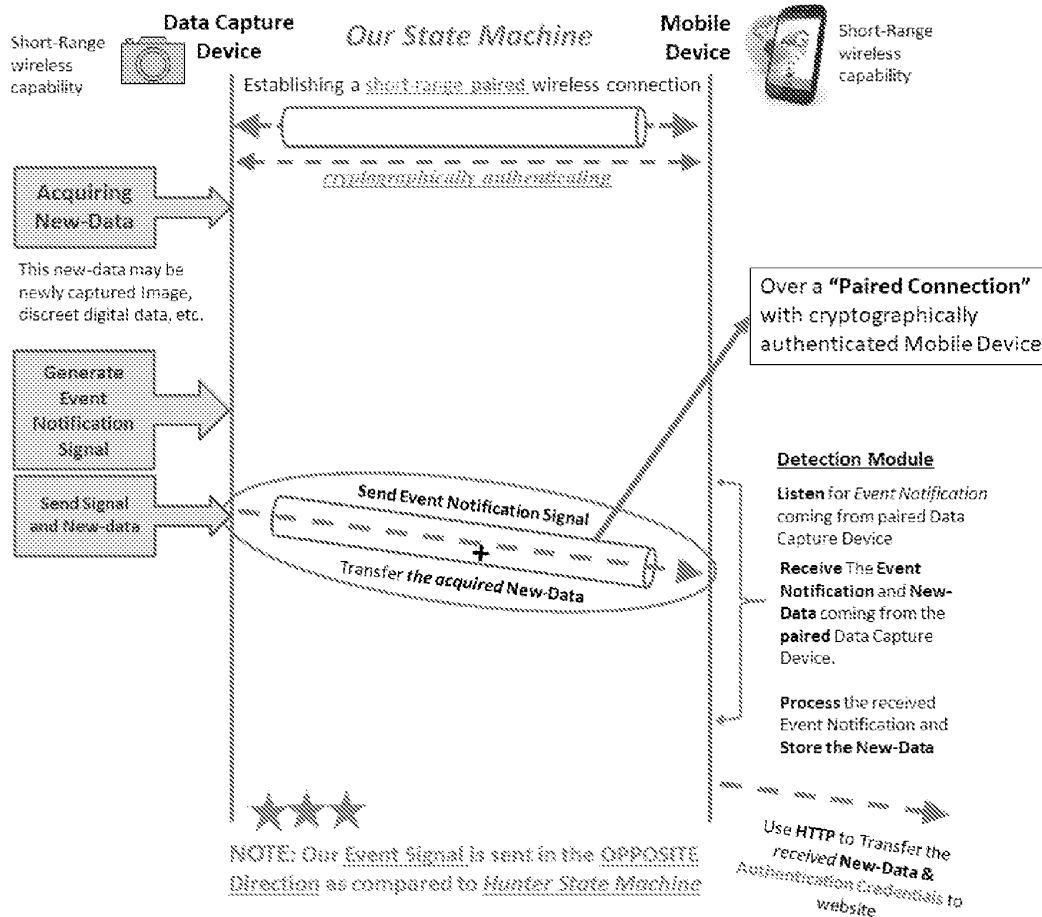
camera. Furthermore, in Hunter, the camera acquires the new-data only after it receives the trigger event or signal from the mobile device. In contrast, in applicant's disclosure, the polling request from the mobile phone to the camera is for detecting already acquired new data.

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 Event Notification signal is sent from sent to the cellular phone. There is NO data capture device.	YES <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</u> pairing is established
6 Data transfer between two devices happens over what type of wireless link?	NON-Paired wireless connection	NO data There is no new- data to transfer	Data over Paired wireless connection

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

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

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

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

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

“a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone, wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled data capture device cryptographically authenticating identity of the short-range wireless enabled cellular phone;”

“said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;”

“said processor further configured to send an event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically, wherein the event notification corresponds to the acquired new-data and comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone, wherein the cryptographically authenticated short-range wireless enabled cellular phone is configured to listen to

the event notification and receive the new-data over the established short-range paired wireless connection, wherein a single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the event notification and store the received new-data in a memory device of the cryptographically authenticated short-range wireless enabled cellular phone, wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone stores a user authentication credential in the memory device of the cryptographically authenticated short-range wireless enabled cellular phone, wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to use HTTP to upload the received new-data and the user authentication credential to a user data publishing website over a cellular data network, wherein the upload is based on a timer setting on the single mobile client application, wherein the timer setting is at least one of no wait automatic, wait X minutes automatic, and wait for user input, and wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data.”

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

“a short-range wireless communication device configured to establish a short-range paired wireless connection between the short-range wireless enabled data capture device and a short-range wireless enabled cellular phone, wherein establishing the short-range paired wireless connection comprises the short-range wireless enabled data capture device cryptographically authenticating identity of the short-range wireless enabled cellular phone;”

“said processor configured to acquire new-data in the short-range wireless enabled data capture device using the data capture circuitry, wherein the new-data is data acquired after establishing the short-range paired wireless connection between the short-range wireless enabled data capture device and the short-range wireless enabled cellular phone;”

“said processor further configured to send an event notification and the acquired new-data to the cryptographically authenticated short-range wireless enabled cellular phone over the established short-range paired wireless connection automatically, wherein the event notification corresponds to the acquired new-data and comprises sending a signal to the cryptographically authenticated short-range wireless enabled cellular phone, wherein the cryptographically authenticated short-range wireless enabled cellular phone is configured to listen to the event notification and receive the new-data over the established short-range paired wireless connection, wherein a single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to process the event notification and store the received new-data in a memory device of the cryptographically authenticated short-range wireless enabled cellular phone, wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone stores a user authentication credential in the memory device of the cryptographically authenticated short-range wireless enabled cellular phone, wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone is configured to use HTTP to upload the received new-data and the user authentication credential to a user data publishing website over a cellular data network, wherein the upload is based on a timer setting on the single mobile client application, wherein the timer setting is at least one of no wait automatic, wait X minutes automatic, and wait for user input, and wherein the single mobile client application for the cryptographically authenticated short-range wireless enabled cellular phone provides a touch based GUI for the received new-data.”

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

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

Conclusion

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re. application of:

Gurvinder Singh

Application No.: 17/542,373

Filed: 12/04/2021

Applicant: CellSpin Soft Inc.

Title: Automatic Multimedia Upload

For Publishing Data And Multimedia Content

Examiner: Nooristany, Sulaiman

Art Unit: 2415

Atty. Docket no.: CellSpin_04Con18

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 October 13, 2022, please see the

Remarks that begin on page 2 of this response.

Remarks

The pending claims

Claims 1-19 are currently pending. Reconsideration and allowance of the pending claims is respectfully requested.

Summary of the Office Action

Double Patenting

Claims 1-19 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claims of Parent Application(s) No. 12333303, 13740214, 14172913, 14273546, 14503401, 14576202, 15659637, 16532507. 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 U.S.C. 112

Claims 1-19 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 display a mobile advertisement inside the mobile software application & touch-based advertisement targeted to a user.

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 "display a mobile advertisement inside the mobile software application" & touch-based advertisement targeted to a user. Appropriate correction is required.

Claim Rejections - 35 USC § 112

Claims 1-19 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 1-3, 5-7 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 4 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.

Claims 8-19 are related to claims 1-7 and are rejected for similar reasons as stated above.

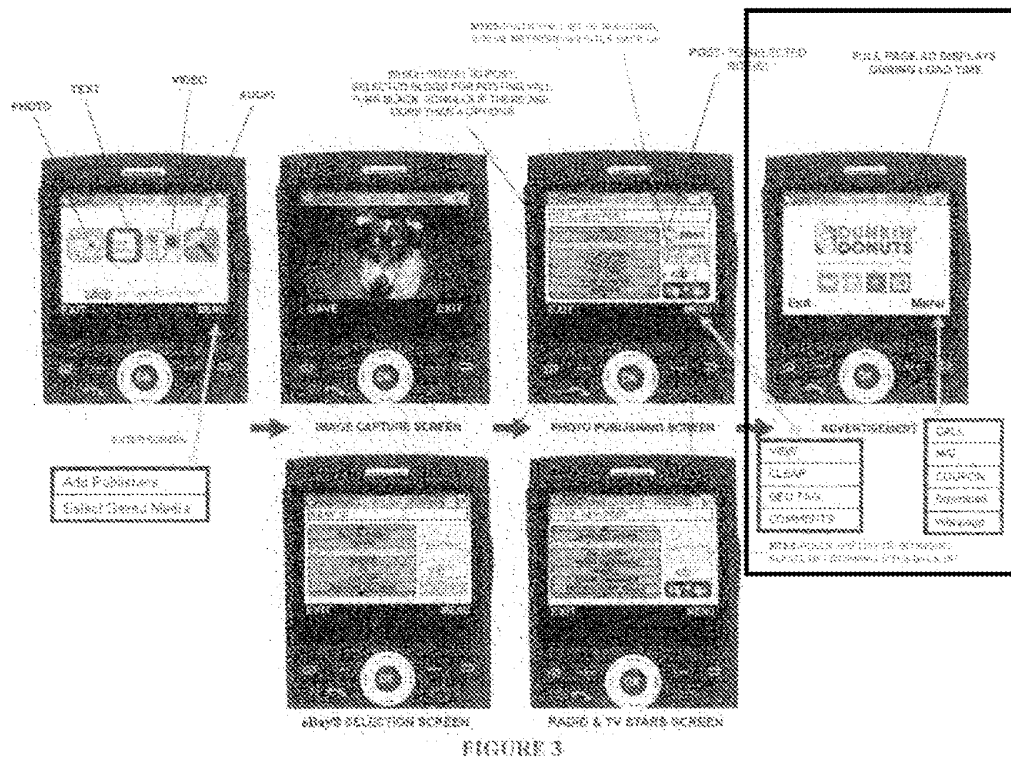
Support for claim limitations

Support for the limitations: “*display a mobile advertisement inside the mobile software application*”, and “*a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application*” in claim 1 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 this response as **Exhibit A** and USPTO Publication No. 2008/0103906 A1 is attached to this response as **Exhibit B**; see also link: <https://patentimages.storage.googleapis.com/1f/06/a0/32f9a69fbef2a6/US20080103906A.pdf>.”

(b) **FIG. 3 of Exhibit B** (reproduced below) Elements **407** and **410**



(c) Paragraph [0021] of **Exhibit B**, which states: “The back end service 204 c may splice the multimedia object with targeted advertisements based on a user profile stored in the database 204 a of the publishing service 204. Also, when the

user 201 is using the client application 202 targeted advertisements may be displayed to the user 201 on the client application 202.”

- (d) FIG. 2, Element 202c, and Paragraph [0032] of Exhibit B, which states: “*a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application*”.
- (e) In Zenon Environmental Inc v. United States Filter Corporation., Nos. 06-1266, - 1267 (Fed. Cir. Nov. 7, 2007), the United States Court of Appeals for the Federal Circuit held that incorporation by reference “*provides a method for integrating material from various documents into a host document . . . by citing such material in a manner that makes clear that the material is effectively part of the host document as if it were explicitly contained therein.*” Cook Biotech Inc. v. Acell, Inc., 460 F.3d 1365, 1376 (Fed. Cir. 2006) (quoting Advanced Display Sys., Inc. v. Kent State Univ., 212 F.3d 1272, 1282 (Fed. Cir. 2000))”.
- (f) Furthermore, in Paice LLC v. Ford Motor Co., 2018 WL 651366 (Fed. Cir. Feb. 1, 2018), Paice’s U.S. Patent No. 7,237,634 (“the ‘634 patent”) claimed priority to U.S. patent application no. 09/264,817 (“the ‘817 application”). A U.S. Patent no. 5,343,970 was incorporated into the ‘817 application: with the following paragraph: “*This application discloses a number of improvements over and enhancements to the hybrid vehicles disclosed in the inventor’s U.S. Pat. No. 5,343,970 (“the ‘970 patent”), which is incorporated herein by this reference. Where differences are not mentioned, it is to be understood that the specifics of the vehicle design shown in the ‘970 patent are applicable to the vehicles shown herein as well.*”

The Federal Circuit noted that the first sentence above broadly and unambiguously states that ‘970 patent is, without qualification, incorporated into the ‘817 application. The Federal Circuit held that the second sentence has no bearing on the

extent of incorporation, and merely states that the features disclosed by ‘970 patent apply to vehicles described as the invention in the ‘817 application, except if the specification mentions otherwise. Citing *Modine Mfg. Co. v. U.S. Int’l Trade Comm’n*, 75 F.3d 1545 (Fed. Cir. 1996), the Federal Circuit stated that “[t]he applicability of a document’s disclosed features and the incorporation of the document itself are distinct concepts, and one does not imply the other.” In summary, the Federal Circuit held that the ‘970 patent is incorporated into the ‘817 patent in its entirety.

In view of the above two Federal circuit decisions, applicant submits that the ‘802 application (application no. 11/901,802, Exhibit A) is incorporated by reference in its entirety in the ‘373 application (application no. 17/542,373).

(g) Furthermore, 37 CFR 1.57 (pre-PLT) – Incorporation by Reference, which is applicable to applications filed before December 18, 2013, provides:

a) Subject to the conditions and requirements of this paragraph, if all or a portion of the specification or drawing(s) is inadvertently omitted from an application, but the application contains a claim under §1.78 for the benefit of a prior-filed provisional, non-provisional, or international application, that was present on the filing date of the application, and the inadvertently omitted portion of the specification or drawing(s) is completely contained in the prior-filed application, the claim under §1.78 shall also be considered an incorporation by reference of the prior-filed application as to the inadvertently omitted portion of the specification or drawing(s).

(1) The application must be amended to include the inadvertently omitted portion of the specification or drawing(s) within any time period set by the Office, but in no case later than the close of prosecution as defined by § 1.114(b), or abandonment of the application, whichever occurs earlier. The applicant is also required to:

- (i) Supply a copy of the prior-filed application, except where the prior-filed application is an application filed under 35 U.S.C. 111;
- (ii) Supply an English language translation of any prior-filed application that is in a language other than English; and
- (iii) Identify where the inadvertently omitted portion of the specification or drawings can be found in the prior-filed application.

Applicant submits that the requirements under 37 CFR 1.57(a) were fulfilled by pending application no. 17/542,373 ('373 application), when the '373 application was filed.

At the time of filing, the '373 application recited on page 2, item 2 of the application that the prior filed application no. 11/901,802 ('802 application, Exhibit A) is incorporated in its entirety in the '373 application.

The '802 application (Exhibit A) was pending, and not abandoned, at the time of filing of the '373 application.

37 CFR 1.57(a)(1)(i) and 37 CFR 1.57(a)(1)(ii) are not applicable to the '802 application (Exhibit A), and since the '802 application (Exhibit A) was incorporated by reference in its entirety in the '373 application, 37 CFR 1.57(a)(1)(iii) is satisfied.

- (h) Enclosed: (a) Copy of pages 1 and 2 of the specification of pending application no. 17/542,373 ('373 application).

Support for claim 6 is found in paragraph [0042] of Exhibit B.

The office action states: “**Claims 1-19 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claims of Parent Application(s) No. 12333303, 13740214, 14172913, 14273546, 14503401, 14576202, 15659637, 16532507. 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 has timely filed a terminal disclaimer to overcome the double patenting rejection. Applicant therefore respectfully requests that the nonstatutory double patenting rejection be reconsidered and withdrawn.

The office action further states: “**Claims 1-19 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 display a mobile advertisement inside the mobile software application & touch-based advertisement targeted to a user.**”

In response to the above rejection, applicant submits that in pages 3-7 of this response, applicant has provided arguments to show that the limitations: “*display a mobile advertisement inside the mobile software application*”, and “*a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application*” are supported in the specification of the current application, because of incorporation in its entirety of 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” into the current application. Therefore, claims 1-19 fully comply with the written description requirement.

Applicant therefore respectfully requests that the rejection of claims 1-19 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 "display a mobile advertisement inside the mobile software application" & touch-based advertisement targeted to a user. Appropriate correction is required.**”

In response to the above objection, applicant submits that in pages 3-7 of this response, applicant has provided arguments to show that the limitations: “*display a mobile advertisement inside the mobile software application*”, and “*a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application*” are supported in the specification of the current application, because of *incorporation in its entirety of 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*” into the current application. Therefore, the above limitations are fully supported in the current specification.

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

The office action further states: “**Claims 1-19 are rejected under 35 USC 112, second paragraph as being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention.**”

Applicant disagrees with the above rejection and presents the following arguments. In pages 3-7 of this response, applicant has provided arguments to show that the limitations: “*display a mobile advertisement inside the mobile software application*”,

and “a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application” are supported in the specification of the current application, because of **incorporation in its entirety** of 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” into the current application. Therefore, claims 1-19 particularly point and distinctly claim the subject matter which applicant regards as the invention.

Applicant, therefore respectfully requests that the rejection of claims 1-19 under 35 U.S.C 112, second paragraph be reconsidered and withdrawn.

The office action further states: “**Claims 1-14 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Hunter US 20040005915 in view of Pietruszka US 20070226778. Claims 8-19 are related to claims 1-7 and are rejected for similar reasons**”.

Argument 1

In response to the above rejection, applicant submits that Hunter, in view of Pietruszka does not teach or suggest the following limitations in claim 1:

“a mobile software application for a Bluetooth enabled cellular phone, wherein the mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, configured to:

display a mobile advertisement inside the mobile software application;”

“a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application;”

“use Hypertext Transfer Protocol to transfer the received new-data along with a user authentication credential to a remote server over a cellular data network;”

“a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application;”

“said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection, wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone;”

Claim 1 discloses a mobile software application for a Bluetooth enabled cellular phone. The mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, configured to display a mobile advertisement inside the mobile software application.

Claim 1 also discloses a mobile software application advertising software module. The mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application.

Claim 1 also discloses that the mobile software application uses Hypertext Transfer Protocol to transfer the received new-data along with a user authentication credential to a remote server over a cellular data network.

Claim 1 also discloses a user authentication software module. The user authentication software module processes the user authentication credential received from the mobile software application.

Hunter and Pietruszka, singly or in combination, do not teach or suggest the above limitations in claim 1.

By way of explanation, applicant submits that in pages 3-7 of this response, applicant has provided arguments to show that the limitations: “*display a mobile advertisement inside the mobile software application*”, and “*a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application*” are supported in the specification of the current application, because of **incorporation in its entirety** of 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” into the current application.

The office action on page 8 states that Paragraph [0025] and FIG. 1, Element 20 of Hunter teach the above limitations in claim 1. Applicant respectfully disagrees and submits the following arguments. FIG. 1, Element 20 of Hunter is a communication device. Furthermore, there is no teaching or suggestion in Paragraph [0025] of Hunter of a mobile software application for a Bluetooth enabled cellular phone, where the mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, configured to display a mobile advertisement inside the mobile software application. Furthermore, there is no teaching or suggestion in Paragraph [0025] of Hunter of a mobile software application advertising

software module, where the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application.

Therefore, Hunter and Pietruszka, singly or in combination, do not teach or suggest the following limitations in claim 1:

“a mobile software application for a Bluetooth enabled cellular phone, wherein the mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, configured to:

display a mobile advertisement inside the mobile software application;”

“a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application;”

Argument 2

Furthermore, applicant submits that the following limitations in claim 1 are also not taught or suggested by Hunter, in view of Pietruszka:

“use Hypertext Transfer Protocol to transfer the received new-data along with a user authentication credential to a remote server over a cellular data network;”

“a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application;”

By way of explanation, paragraph [0037] of Pietruszka discloses cryptographically authenticating a short-range wireless device. In contrast, applicant's claim 1 recites transferring and processing of a user authentication credential. The user authentication credential is for a website user and NOT for short-range wireless device.

Therefore, applicant submits that "*Cryptographic authentication of a wireless device*" in Pietruszka is not the same as "*transferring and processing of a user authentication credential*" 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 and by *two devices* such as a camera and a mobile phone.

Note: See extract of paragraph [0037] of Pietruszka:

[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.

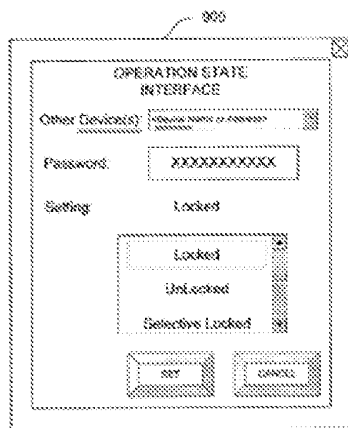


FIG. 9A

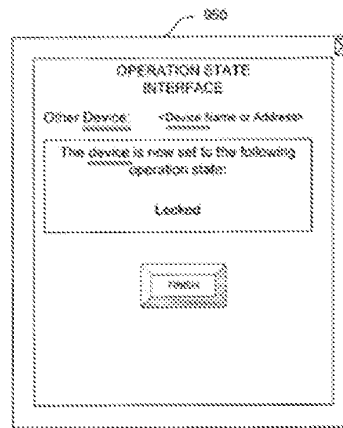


FIG. 9B

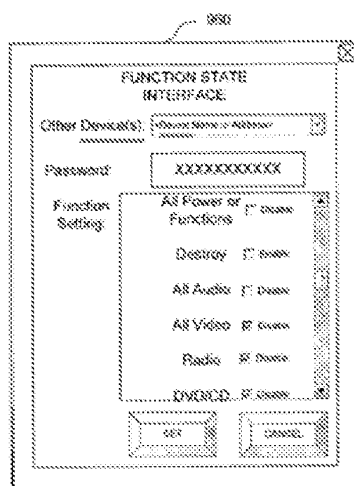


FIG. 9C

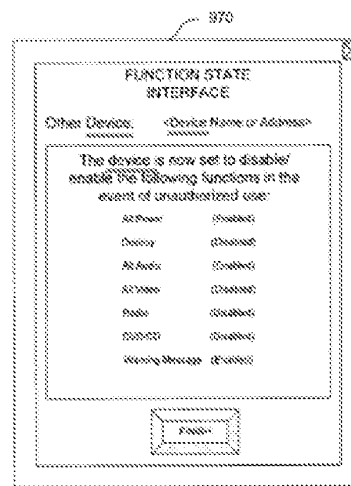


FIG. 9D

- **Pietruszka [0037] is talking about cryptographically authenticating a short-range wireless device. Our Claim is about transferring and processing of website “user” authentication credentials!**
- **Pietruszka [Fig 9A – 9D] make it clear that the authentication is for the Device and NOT for a website user**

Cryptographic authentication of a wireless device



Website user authentication credentials

Furthermore, neither Hunter nor Pietruszka teach or suggest the use of HTTP to transfer the new-data and the user authentication credential to the website. Therefore, even if Hunter and Pietruszka are combined as suggested in the office action, the combination will not teach or suggest the following limitations in claim 1:

“use Hypertext Transfer Protocol to transfer the received new-data along with a user authentication credential to a remote server over a cellular data network;”

“a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application;”

Therefore, the following limitations in claim 1 are also not taught or suggested by Hunter, in view of Pietruszka:

“a mobile software application for a Bluetooth enabled cellular phone, wherein the mobile software application is embodied as executable program instructions

that, when executed by a processor of the Bluetooth enabled cellular phone, configured to:

display a mobile advertisement inside the mobile software application;”

“a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application;”

“use Hypertext Transfer Protocol to transfer the received new-data along with a user authentication credential to a remote server over a cellular data network;”

“a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application;”

Argument 3

Furthermore, applicant submits that the following limitations in claim 1 are also not taught or suggested by Hunter, in view of Pietruszka:

“said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection, wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone;”

The office action on page 6 states that paragraph [0013] of Hunter teaches the above limitation in claim 1.

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*.

The screenshot shows the Oxford English Dictionary entry for the verb 'recognize'. It includes the phonetic transcription /ˈrɛkəg.nɪz/, the part of speech 'verb', and the gerund or present participle 'recognizing'. Two definitions are provided: 1. 'identify (someone or something) from having encountered them before; know again.' with the example 'I recognized her when her wig fell off.' and 2. 'acknowledge the existence, validity, or legality of.' with the example 'the defense is recognized in Mexican law'. Below the definitions is a 'Similar:' section with buttons for 'acknowledge', 'accept', 'admit', 'concede', 'allow', 'grant', and 'confess'. The 'accept' button is highlighted with a red underline. At the bottom, it says '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:

wherein detecting and receiving new-data acquired in the Bluetooth enabled data capture device comprises: said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification (**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]**)).

sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection, wherein the event notification corresponds to the acquired new-data and

Therefore, even if Hunter and Pietruszka are combined as suggested in the office action, the combination will not teach or suggest the following limitations in claim 1:

“said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection, wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone;”

Argument 4

Furthermore, Hunter does not teach establishment of a paired Bluetooth connection. Applicant provides the following arguments to illustrate this.

Establishment of non-paired connection (Hunter)

versus

Establishment of paired Bluetooth connection (Applicant)

The office action on page 6 states that Hunter teaches the step of acquiring new-data after establishing the paired Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone. Applicant respectfully disagrees and presents the following arguments.

Hunter prior art does NOT teach pairing or paired connection. There is NO disclosure or recitation of the word pair, pairing, or paired in the Hunter specification.

Argument 5

Furthermore, applicant submits that there is no phone call trigger event in applicant's invention. By way of arguments:

Receiving or making Phone call trigger event (Hunter)

versus

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 paired Bluetooth connection between the Bluetooth enabled data capture device and the Bluetooth enabled cellular phone. Applicant respectfully disagrees and presents the following arguments.

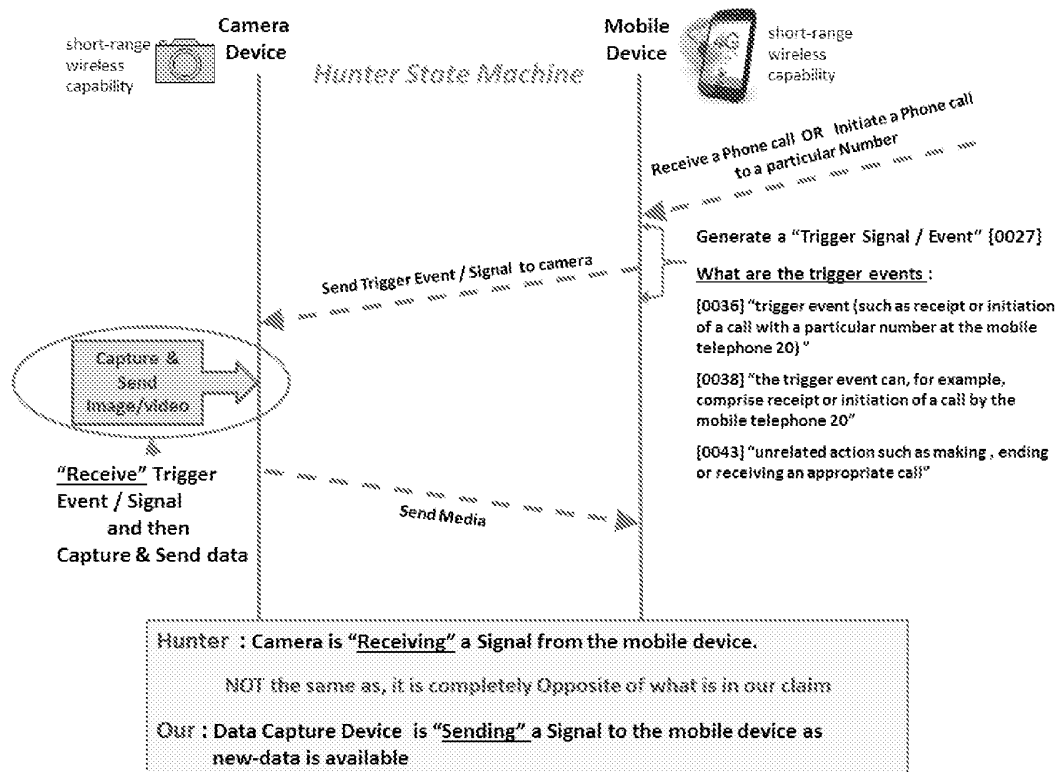
The sequence of events in Hunter is as follows:

- (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) Sends 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.

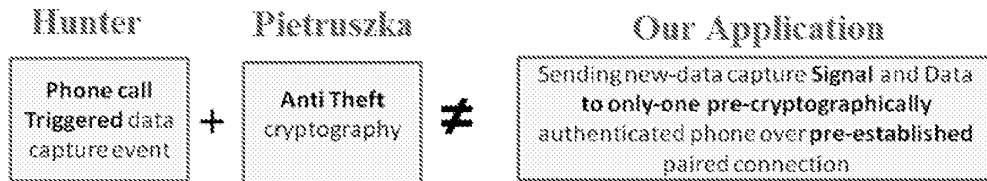
Next, in Hunter, the data capture device acquires new-data only after it receives the trigger event or signal from the mobile device. This is in direct contrast to applicant's disclosure where a data capture device acquires new-data after a paired Bluetooth wireless connection is established with a cellular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



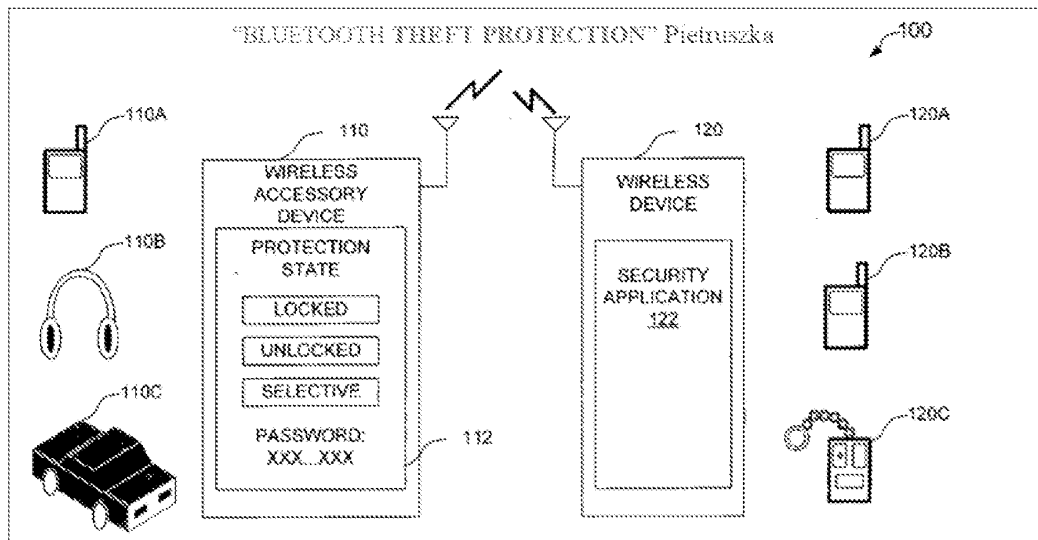
Argument 6

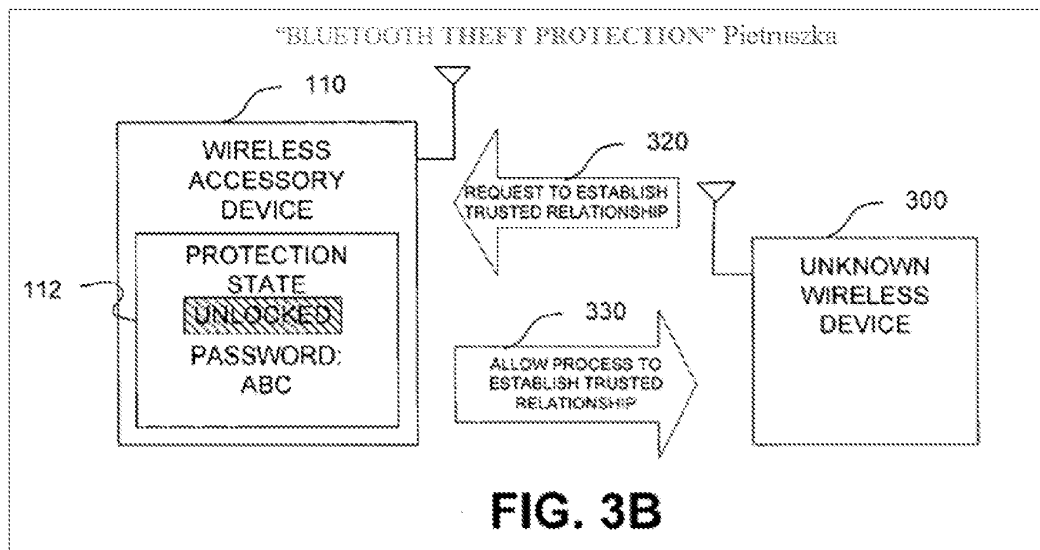
Furthermore, there is no motivation to combine (i) Phone call triggered data capture event of Hunter with (ii) the Anti-Theft Pietruszka teaching.



Anti-theft setting-based control of cryptographic pairing between devices in Pietruszka is not relevant in applicant's scenario. By way of arguments:

**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 inter alia 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 inter alia 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 paired Bluetooth wireless connection. Pietruszka's invention pertains primarily to theft protection based on pre-set operational state of the device in its proximity.

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

Argument 7

Furthermore, applicant submits that the following limitation in claim 1 is also not taught or suggested by Hunter, in view of Pietruszka:

"wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone;"

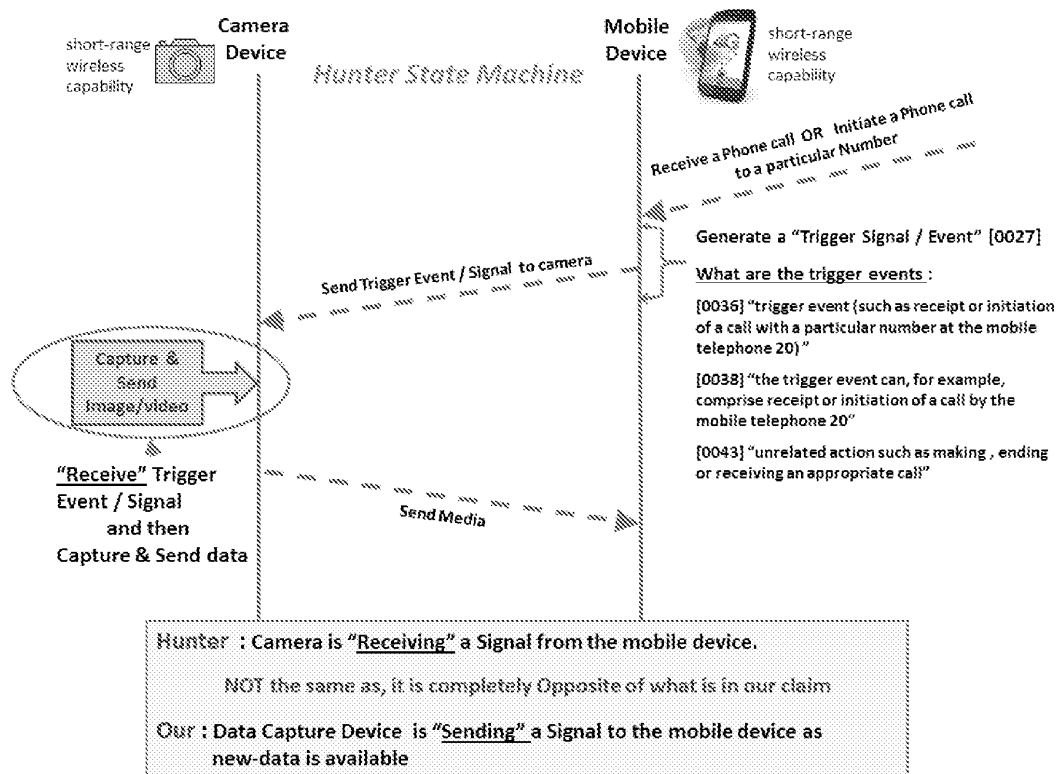
By way of explanation, applicant submits the following arguments:

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

The office action on page 7 states that paragraph [0013] of Hunter teaches: “receiving an event notification by the cryptographically authenticated Bluetooth enabled cellular phone”. Applicant respectfully 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]:



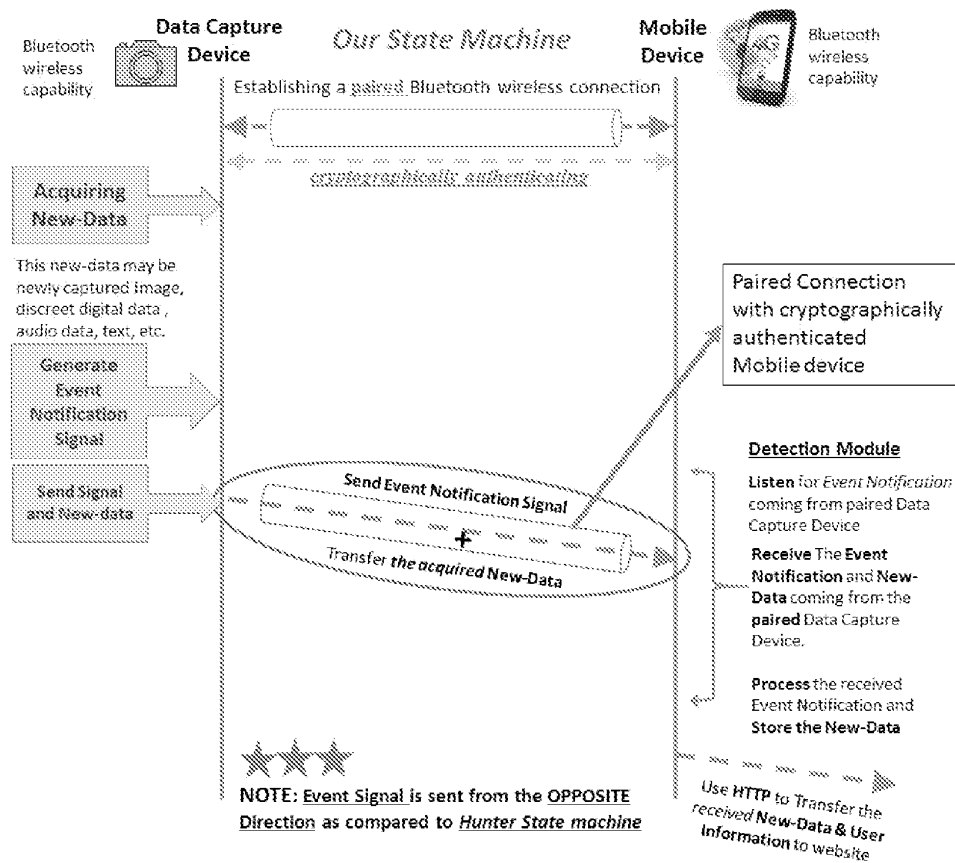
First, in Hunter, there is NO cryptographic authentication of the mobile device by the data capture device before the signal is sent or the data is sent. Next, in Hunter, receipt of a phone call or an outgoing phone call is required for the mobile device to generate a trigger event or signal to be sent 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 Bluetooth enabled data capture device acquires new-data after a Bluetooth connection is established with a cellular phone (without any phone call trigger event from the Bluetooth enabled cellular phone to the Bluetooth enabled data capture device).

Next, in Hunter, the phone call trigger event is sent from the mobile device to the data capture device. An event signal is sent in the opposite direction when compared to

the applicants claims. The direction of the 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 Bluetooth enabled data capture device acquires new-data immediately after the paired Bluetooth 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 Bluetooth enabled data capture device sends the notification signal to the Bluetooth enabled mobile device informing the Bluetooth enabled mobile device that it has acquired the new-data.

Therefore, applicant submits that the following limitation in claim 1 is also not taught or suggested by Hunter, in view of Pietruszka:

“wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone;”

Argument 8

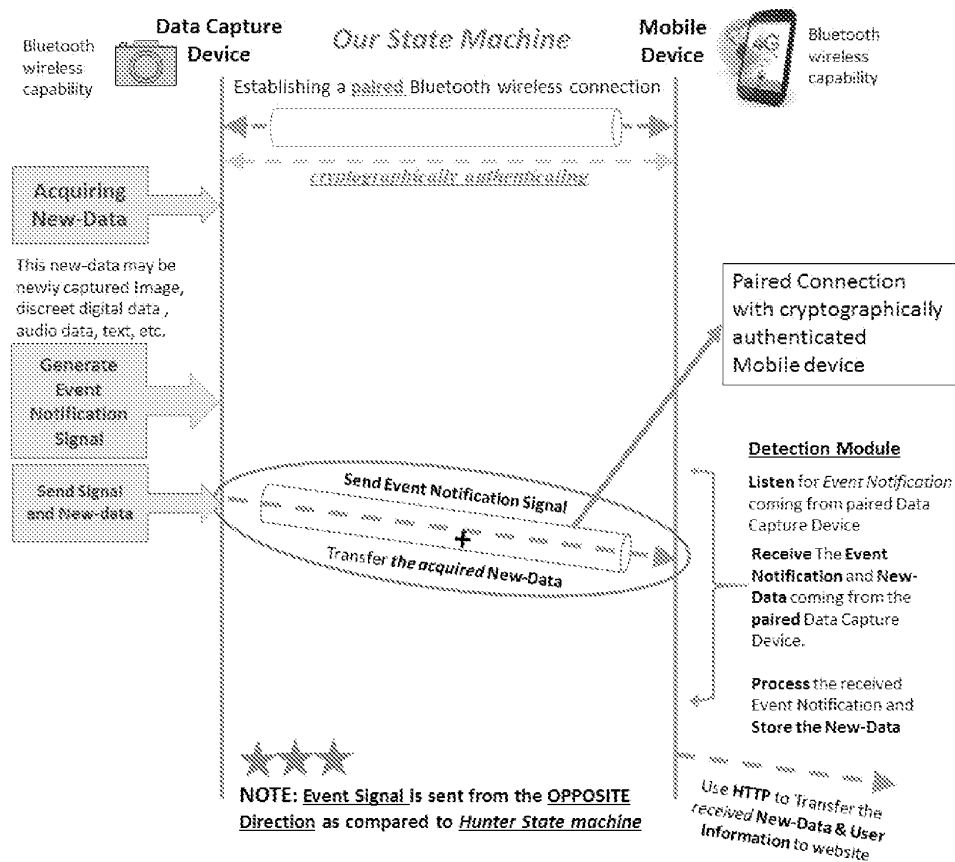
Furthermore, the phone call Trigger event in Hunter (see paragraphs [0036], [0038], [0043]) is over a NON paired connection. By way of explanation:

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 Bluetooth connection is established, without any phone call trigger event from the Bluetooth enabled 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.

Summary

Applicant's state machine



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

In view of the arguments presented above, the following limitations in claim 1 are not taught or suggested by Hunter, in view of Pietruszka:

“a mobile software application for a Bluetooth enabled cellular phone, wherein the mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, configured to:

display a mobile advertisement inside the mobile software application;”

“a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application;”

“use Hypertext Transfer Protocol to transfer the received new-data along with a user authentication credential to a remote server over a cellular data network;”

“a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application;”

“said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection, wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone;”

Claim 1 is therefore non-obvious over Hunter, in view of Pietruszka. Applicant therefore respectfully requests that the rejection of claim 1 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

Argument 9

Claim 8 is analogous to claim 1. Since claim 1 is non-obvious over Hunter, in view of Pietruszka, applicant respectfully submits claim 8 is also non-obvious over Hunter, in view of Pietruszka. Applicant therefore respectfully requests that the rejection of claim 8 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

Furthermore, claim 14 is analogous to claim 1. In addition, the following limitation in claim 14 is not taught or suggested by Hunter, in view of Pietruszka:

“said mobile software application for the Bluetooth enabled cellular phone configured to poll the Bluetooth enabled data capture device for new-data, over the established paired Bluetooth connection, wherein polling comprises sending a request to the Bluetooth enabled data capture device to check if the acquired new-data is available for transfer;”

In claim 14, the Bluetooth enabled cellular phone sends a polling request to the Bluetooth enabled data capture device, over an established paired Bluetooth connection, to detect new-data for transfer from the paired Bluetooth connection to the paired and cryptographically authenticated Bluetooth 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 argument presented above, applicant submits that Hunter, in view of Pietruszka does not teach or suggest the following limitation in claim 14:

“said mobile software application for the Bluetooth enabled cellular phone configured to poll the Bluetooth enabled data capture device for new-data, over the established paired Bluetooth connection, wherein polling comprises sending a request to the Bluetooth enabled data capture device to check if the acquired new-data is available for transfer;”

Therefore, claim 14 is non-obvious over Hunter, in view of Pietruszka. Applicant therefore respectfully requests that the rejection of claim 14 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

Argument 10

Claims 2-3 and 5-7 are dependent on claim 1. Claims 9-13 are dependent on claim 8. Claims 15-19 are dependent on claim 14. Since claims 1, 8 and 14 are non-obvious over Hunter, in view of Pietruszka, claims 2-3, 5-7, 9-13 and 15-19 are also non-obvious over Hunter, in view of Pietruszka. Applicant therefore respectfully requests that the rejection of claims 2-3, 5-7, 9-13 and 15-19 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

The office action further states: **“Claim 4 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 illustrate that Hunter, in view of Pietruszka does not teach or suggest the following limitations in claim 1:

“a mobile software application for a Bluetooth enabled cellular phone, wherein the mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, configured to:

display a mobile advertisement inside the mobile software application;”

“a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application;”

“use Hypertext Transfer Protocol to transfer the received new-data along with a user authentication credential to a remote server over a cellular data network;”

“a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application;”

“said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection, wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone;”

Risbood does not remedy the deficiencies in a combination of Hunter and Pietruszka. Therefore, Hunter, in view of Pietruszka, further in view of Risbood, does not teach or suggest the following limitations in claim 1:

“a mobile software application for a Bluetooth enabled cellular phone, wherein the mobile software application is embodied as executable program instructions that, when executed by a processor of the Bluetooth enabled cellular phone, configured to:

display a mobile advertisement inside the mobile software application;”

“a mobile software application advertising software module, wherein the mobile software application advertising software module selects advertisements based on the user profile and sends the selected advertisements to the mobile software application;”

“use Hypertext Transfer Protocol to transfer the received new-data along with a user authentication credential to a remote server over a cellular data network;”

“a user authentication software module, wherein the user authentication software module processes the user authentication credential received from the mobile software application;”

“said mobile software application for the Bluetooth enabled cellular phone configured to listen for an event notification, sent from the Bluetooth enabled data capture device, over the established paired Bluetooth connection, wherein the event notification corresponds to the acquired new-data and comprises sending a signal from the Bluetooth enabled data capture device to the Bluetooth enabled cellular phone;”

Therefore, even if Hunter, Pietruszka and Risbood are combined as suggested in the office action, the combination will not teach or suggest the above limitations in claim 1. Claim 1 is therefore non-obvious over Hunter, in view of Pietruszka, further in view of Risbood. Applicant therefore respectfully requests that the rejection of claim 1 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

Claim 4 is dependent on claim 1. Since claim 1 is non-obvious over Hunter, in view of Pietruszka, further in view of Risbood, claim 4 is also non-obvious over Hunter, in view of Pietruszka, further in view of Risbood. Applicant therefore respectfully requests that the rejection of claim 4 under pre-AIA 35 U.S.C. 103(a) be reconsidered and withdrawn.

Conclusion

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

Respectfully submitted,

Date: January 09, 2023

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

Correspondence Address

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