



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.
17/943,956	27-JUN-23	11689383

BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX)
TWO NORTH CENTRAL AVENUE, SUITE 2100
PHOENIX, AZ 85004

EGRANT NOTIFICATION

Your electronic patent grant (eGrant) is now available, which can be accessed via Patent Center at <https://patentcenter.uspto.gov>

The electronic patent grant is the official patent grant under 35 U.S.C. 153. For more information, please visit <https://www.uspto.gov/electronicgrants>



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/943,956	06/27/2023	11689383	3010043.2	2316

46019 7590 06/07/2023
BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX)
TWO NORTH CENTRAL AVENUE, SUITE 2100
PHOENIX, AZ 85004

ISSUE NOTIFICATION

The projected patent number and issue date are specified above. The patent will issue electronically. The electronically issued patent is the official patent grant pursuant to 35 U.S.C. § 153. The patent may be accessed on or after the issue date through Patent Center at <https://patentcenter.uspto.gov/>. The patent will be available in both the public and the private sides of Patent Center. Further assistance in electronically accessing the patent, or about Patent Center, is available by calling the Patent Electronic Business Center at 1-888-217-9197.

The USPTO is implementing electronic patent issuance with a transition period, during which period the USPTO will mail a ceremonial paper copy of the electronic patent grant to the correspondence address of record. Additional copies of the patent (i.e., certified and presentation copies) may be ordered for a fee from the USPTO's Certified Copy Center at <https://certifiedcopycenter.uspto.gov/index.html>. The Certified Copy Center may be reached at (800)972-6382.

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

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Patents Stakeholder Experience (OPSE), Stakeholder Support Division (SSD) at (571)-272-4200.

INVENTOR(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional inventors):

Alexander Dizengof, Ashdod, ISRAEL;

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Carbyne Ltd., Tel-Aviv, ISRAEL;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17943956	
	Filing Date		2022-09-13	
	First Named Inventor	Alexander Dizengof		
	Art Unit	2646		
	Examiner Name	Lafontant, Gary		
	Attorney Docket Number	3010043.2		

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ^{2]}	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2992692	EU EP		2016-03-09	Decharms		

Change(s) applied to document /P.P./

If you wish to add additional Foreign Patent Document citation information please click the Add button.

NON-PATENT LITERATURE DOCUMENTS

5/1/2023

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	European Search Report and the European Search Opinion Dated 08 April 2022 from the European Patent Office Re. Application No. 22152510.8, (11 Pages).	
	2	European Search Report and the European Search Opinion Dated 06 December 2018 from the European Patent Office Re. Application No. 18188748.0, (10 Pages).	

If you wish to add additional non-patent literature document citation information please click the Add button.

EXAMINER SIGNATURE

Examiner Signature	/GARY LAFONTANT/	Date Considered	03/08/2023
--------------------	------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #
17/943,956

RECEIPT DATE / TIME
05/09/2023 06:09:58 PM ET

ATTORNEY DOCKET #
3010043.2

Title of Invention

SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	2316	FILED BY	Julie Eslick
PATENT CENTER #	62064034	FILING DATE	09/13/2022
CUSTOMER #	46019	FIRST NAMED INVENTOR	Alexander Dizengof
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Cory Smith

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
000002-IFT-signed.pdf	1	Issue Fee Payment (PTO-85B)	231 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
000002-IFT-signed.pdf	C955B4BEEF42132082139373228B2C03CC8616A9367A78C4EB DD1534B2AF2AA70E48306791229657DB684385964ACB20EB77 C7A0084D0650C6488A75744A2A89

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized

by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PART B - FEE(S) TRANSMITTAL

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

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

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

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

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

46019 7590 04/27/2023

BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX)
TWO NORTH CENTRAL AVENUE, SUITE 2100
PHOENIX, AZ 85004

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

Certificate of Mailing or Transmission

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

Julie A. Eslick	(Typed or printed name)
/Julie A. Eslick/	(Signature)
May 9, 2023	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/943,956	09/13/2022	Alexander Dizengof	3010043.2	2316

TITLE OF INVENTION: SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0.00	\$0.00	\$480	07/27/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
LAFONTANT, GARY	2646	455-404200

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

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

"Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

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

BRYAN CAVE LEIGHTON
PAISNER LLP

- 1 _____
- 2 _____
- 3 _____

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

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

(A) NAME OF ASSIGNEE
CARBYNE LTD.

(B) RESIDENCE: (CITY and STATE OR COUNTRY)
TEL-AVIV, ISRAEL

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

4a. Fees submitted: Issue Fee Publication Fee (if required)

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

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

The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 024467

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

Applicant certifying micro entity status. See 37 CFR 1.29

Applicant asserting small entity status. See 37 CFR 1.27

Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature /Cory Smith/ Date May 9, 2023
Typed or printed name Cory Smith Registration No. 63218



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #
17/943,956

RECEIPT DATE / TIME
05/09/2023 06:09:58 PM ET

ATTORNEY DOCKET #
3010043.2

Title of Invention

SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	2316	FILED BY	Julie Eslick
PATENT CENTER #	62064034	AUTHORIZED BY	Cory Smith
CUSTOMER #	46019	FILING DATE	09/13/2022
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Alexander Dizengof

Payment Information

PAYMENT METHOD
DA / 024467

PAYMENT TRANSACTION ID
E20235911158627

PAYMENT AUTHORIZED BY
Julie Eslick

PRE-AUTHORIZED ACCOUNT
024467

PRE-AUTHORIZED CATEGORY
37 CFR 1.16 (National application filing, search, and examination fees); 37 CFR 1.17 (Patent application and reexamination processing fees); 37 CFR 1.19 (Document supply fees); 37 CFR 1.20 (Post issuance fees); 37 CFR 1.21 (Miscellaneous fees and charges)

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
2501	UTILITY ISSUE FEE	480.00	1	480.00
TOTAL AMOUNT:				\$480.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d))

and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/943,956	09/13/2022	Alexander Dizengof	3010043.2	2316
46019	7590	05/01/2023	EXAMINER LAFONTANT, GARY	
BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX) TWO NORTH CENTRAL AVENUE, SUITE 2100 PHOENIX, AZ 85004			ART UNIT PAPER NUMBER 2646	
			NOTIFICATION DATE DELIVERY MODE 05/01/2023 ELECTRONIC	

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

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

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

PXBCIPDocketing@bcplaw.com

<i>Decision Granting Request for Prioritized Examination (Track I)</i>	Application No. 17/943,956	Applicant(s) Dizengof, Alexander	
	Examiner JoAnne L Burke	Art Unit OPET	AIA (FITF) Status Yes
<p>1. THE REQUEST FILED <u>17 April 2023</u> IS GRANTED .</p> <p>The above-identified application has met the requirements for prioritized examination</p> <p>A. <input type="checkbox"/> for an original nonprovisional application (Track I).</p> <p>B. <input checked="" type="checkbox"/> for an application undergoing continued examination (RCE).</p> <p>2. The above-identified application will undergo prioritized examination. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:</p> <p>A. filing a <u>petition for extension of time</u> to extend the time period for filing a reply;</p> <p>B. filing an <u>amendment to amend the application to contain more than four independent claims, more than thirty total claims</u>, or a multiple dependent claim;</p> <p>C. filing a <u>request for continued examination</u> ;</p> <p>D. filing a notice of appeal;</p> <p>E. filing a request for suspension of action;</p> <p>F. mailing of a notice of allowance;</p> <p>G. mailing of a final Office action;</p> <p>H. completion of examination as defined in 37 CFR 41.102; or</p> <p>I. abandonment of the application.</p> <p>Telephone inquiries with regard to this decision should be directed to JoAnne Burke at (571)272-4584. In his/her absence, calls may be directed to Petition Help Desk at (571) 272-3282.</p>			
/JOANNE L BURKE/ Lead Paralegal Specialist, OPET			



United States Patent and Trademark Office

Office of the Chief Financial Officer

Document Code:WFEE

User :Gloria Arias

Sale Accounting Date:04/28/2023

Sale Item Reference Number	Effective Date
17943956	04/17/2023

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method
I20234RE17327276	2830	PROCESSING FEE, EXCEPT PROV. APPLS.	\$56.00	Deposit Account



UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

46019 7590 04/27/2023
BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX)
TWO NORTH CENTRAL AVENUE, SUITE 2100
PHOENIX, AZ 85004

EXAMINER

LAFONTANT, GARY

ART UNIT PAPER NUMBER

2646

DATE MAILED: 04/27/2023

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Values: 17/943,956, 09/13/2022, Alexander Dizengof, 3010043.2, 2316

TITLE OF INVENTION: SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE

Table with 7 columns: APPLN. TYPE, ENTITY STATUS, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE. Values: nonprovisional, SMALL, \$480, \$0.00, \$0.00, \$480, 07/27/2023

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

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

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

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

PART B - FEE(S) TRANSMITTAL

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

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

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

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

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

46019 7590 04/27/2023

BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX)
 TWO NORTH CENTRAL AVENUE, SUITE 2100
 PHOENIX, AZ 85004

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

Certificate of Mailing or Transmission

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/943,956	09/13/2022	Alexander Dizengof	3010043.2	2316

TITLE OF INVENTION: SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0.00	\$0.00	\$480	07/27/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
LAFONTANT, GARY	2646	455-404200

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

- Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.
- "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

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

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

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

(A) NAME OF ASSIGNEE _____

(B) RESIDENCE: (CITY and STATE OR COUNTRY) _____

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

4a. Fees submitted: Issue Fee Publication Fee (if required)

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

- Electronic Payment via Patent Center or EFS-Web Enclosed check Non-electronic payment by credit card (Attach form PTO-2038)
- The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

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

- Applicant certifying micro entity status. See 37 CFR 1.29
- Applicant asserting small entity status. See 37 CFR 1.27
- Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes details for application 17/943,956, inventor Alexander Dizengof, and examiner GARY LAFONTANT.

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

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

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702.

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

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

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

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 17/943,956	Applicant(s) Dizengof, Alexander	
	Examiner GARY LAFONTANT	Art Unit 2646	AIA (FITF) Status Yes

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

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

1. This communication is responsive to claim submission 04/17/23.
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
2. An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. The allowed claim(s) is/are 1-20. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) All b) Some* c) None of the:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Examiner's Amendment/Comment |
| 2. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____. | 6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| 3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material _____. | 7. <input type="checkbox"/> Other _____. |
| 4. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. | |

/GARY LAFONTANT/
Examiner, Art Unit 2646

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Continued Examination Under 37 CFR 1.114.

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **04/17/2023** has been entered.

Receipt is acknowledged of amendments/arguments filed on **04/17/2023**.

Claims 1-20 are presented for examination.

Allowable Subject Matter

Claims 1-20 are allowed.

The following is an examiner's statement of reasons for allowance:

Independent **claims 1, 8 and 15** are allowable in view of applicant 's arguments and primary reference **Piett (US 2016/0337831 A1)** considered to be closed to the applicant subject matter, does not teach the following limitation:

“wherein the real-time video stream is received through the WebRTC session while audio content of the emergency call is received through the first connection”.

Therefore, **Claims 1-20** are considered novel and non-obvious and are therefore allowed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to GARY LAFONTANT whose telephone number is (571)272-3037. The examiner can normally be reached on 9:00AM -5:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lester Kincaid can be reached on 571-272-7922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


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

Application/Control Number: 17/943,956
Art Unit: 2646

Page 5

/GARY LAFONTANT/

Examiner, Art Unit 2646

<i>Search Notes</i> 	Application/Control No. 17/943,956	Applicant(s)/Patent Under Reexamination Dizengof, Alexander
	Examiner GARY LAFONTANT	Art Unit 2646

CPC - Searched*		
Symbol	Date	Examiner
All	11/18/2022	GL
ALL	03/08/2023	GL
ALL	04/22/2023	GL

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

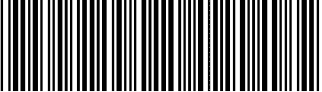
US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Pe2E Searh	11/18/2022	GL
PE2E Search	03/08/2023	GL
PE2E SEARCH	04/22/2023	GL

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
SAME AS ABOVE	SAME AS ABOVE	04/22/2023	GL

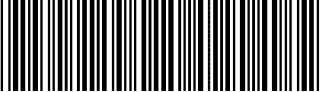
/GARY LAFONTANT/ Examiner, Art Unit 2646	
---	--

Issue Classification 	Application/Control No. 17/943,956	Applicant(s)/Patent Under Reexamination Dizengof, Alexander
	Examiner GARY LAFONTANT	Art Unit 2646

CPC						
Symbol					Type	Version
H04L	/	12	/	1895	F	2013-01-01
H04L	/	41	/	0654	I	2013-01-01
H04M	/	3	/	5116	I	2013-01-01
H04L	/	67	/	146	I	2013-01-01
H04L	/	65	/	1046	I	2013-01-01
H04L	/	65	/	1053	I	2013-01-01
H04L	/	65	/	1069	I	2013-01-01
H04W	/	4	/	90	I	2018-02-01
H04L	/	65	/	1096	I	2013-01-01
H04M	/	1	/	72418	I	2021-01-01
H04M	/	2242	/	15	A	2013-01-01
H04W	/	4	/	14	A	2013-01-01
H04W	/	76	/	19	A	2018-02-01
H04W	/	4	/	027	A	2013-01-01

CPC Combination Sets				
Symbol	Type	Set	Ranking	Version
/	/	/	/	/

NONE	Total Claims Allowed:	
(Assistant Examiner)	(Date)	20
/GARY LAFONTANT/ Examiner, Art Unit 2646	22 April 2023	O.G. Print Claim(s)
(Primary Examiner)	(Date)	1
		O.G. Print Figure
		1

Issue Classification 	Application/Control No. 17/943,956	Applicant(s)/Patent Under Reexamination Dizengof, Alexander
	Examiner GARY LAFONTANT	Art Unit 2646

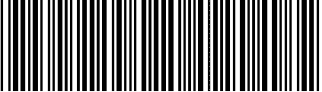
INTERNATIONAL CLASSIFICATION			
CLAIMED			
H04M		3	42

NON-CLAIMED			

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					


NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/GARY LAFONTANT/ Examiner, Art Unit 2646	22 April 2023	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification 	Application/Control No. 17/943,956	Applicant(s)/Patent Under Reexamination Dizengof, Alexander
	Examiner GARY LAFONTANT	Art Unit 2646

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		10		19										
	2		11		20										
	3		12												
	4		13												
	5		14												
	6		15												
	7		16												
	8		17												
	9		18												

NONE	Total Claims Allowed:	
(Assistant Examiner)	(Date)	20
/GARY LAFONTANT/ Examiner, Art Unit 2646	22 April 2023	O.G. Print Claim(s)
(Primary Examiner)	(Date)	O.G. Print Figure
		1
		1

<i>Index of Claims</i> 	Application/Control No. 17/943,956	Applicant(s)/Patent Under Reexamination Dizengof, Alexander
	Examiner GARY LAFONTANT	Art Unit 2646

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

CLAIMS									
<input checked="" type="checkbox"/> Claims renumbered in the same order as presented by applicant <input type="checkbox"/> CPA <input type="checkbox"/> T.D. <input type="checkbox"/> R.1.47									
CLAIM		DATE							
Final	Original	11/18/2022	03/08/2023	04/22/2023					
	1	✓	✓	=					
	2	✓	✓	=					
	3	✓	✓	=					
	4	✓	✓	=					
	5	✓	✓	=					
	6	✓	✓	=					
	7	✓	✓	=					
	8	✓	✓	=					
	9	✓	✓	=					
	10	✓	✓	=					
	11	✓	✓	=					
	12	✓	✓	=					
	13	✓	✓	=					
	14	✓	✓	=					
	15	✓	✓	=					
	16	✓	✓	=					
	17	✓	✓	=					
	18	✓	✓	=					
	19	✓	✓	=					
	20	✓	✓	=					

Bibliographic Data

Application No: 17/943,956

Foreign Priority claimed: Yes No

35 USC 119 (a-d) conditions met: Yes No Met After Allowance

Verified and Acknowledged: /GARY LAFONTANT/

G.L

Examiner's Signature

Initials

Title:

SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM
FOR STREAMING REAL-TIME DATA FROM A USER DEVICE

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/13/2022	455	2646	3010043.2
RULE			

APPLICANTS

Carbyne Ltd.,

INVENTORS

Alexander Dizengof, Ashdod, ISRAEL

CONTINUING DATA

This application is a CON of 17492757 10/04/2021

17492757 is a CON of 16901074 06/15/2020 PAT 11139996

16901074 is a CON of 15822927 11/27/2017 PAT 10686618

15822927 has PRO of 62544835 08/13/2017

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

09/28/2022

** SMALL ENTITY **

STATE OR COUNTRY

ISRAEL

ADDRESS

BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX)

TWO NORTH CENTRAL AVENUE, SUITE 2100

PHOENIX, AZ 85004

UNITED STATES

FILING FEE RECEIVED

\$3,000

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	8	"20150106528"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/11/18 04:21 PM
L2	2	"20150106528"	(US-PGPUB; USPAT)	OR	ON	ON	2022/11/18 04:21 PM
L3	2	"20160337831"	(US-PGPUB; USPAT)	OR	ON	ON	2022/11/18 04:22 PM
L4	0	(URL ADJ2 link) NEAR9 WebRTC AND @ad<"20170813"	(DERWENT)	OR	ON	ON	2023/02/28 06:05 PM
L5	2	(URL ADJ2 link) NEAR9 WebRTC AND @ad<"20170813"	(USPAT)	OR	ON	ON	2023/02/28 06:05 PM
L6	1	((URL OR (uniform ADJ2 resource ADJ2 locator)) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(DERWENT)	OR	ON	ON	2023/03/01 12:46 AM
L7	1	((URL OR (uniform ADJ2 resource ADJ2 locator)) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) SAME2 (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(DERWENT)	OR	ON	ON	2023/03/01 12:47 AM
L8	3	((URL OR (uniform ADJ2 resource ADJ2 locator)) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) SAME2 (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 12:47 AM
L9	5	((URL OR (uniform ADJ2 resource ADJ2	(US-PGPUB; USPAT; USOCR; FIT (AU, AP,	OR	ON	ON	2023/03/01 01:11 AM

L10	20	locator)) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) AND (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 01:14 AM
L11	1265	((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 01:32 AM
L12	6	((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) AND (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 01:33 AM
L13	6	((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web OR IP OR (internet ADJ2 protocol)) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) AND (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 12:41 PM
L14	562	((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web OR IP OR (internet ADJ2 protocol))) NEAR9 ((phone OR telephone) NEAR2 number) AND (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication))	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 12:41 PM

L15	107	AND @ad<"20170813" ((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web OR IP OR (internet ADJ2 protocol))) NEAR9 ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 12:42 PM
L16	3	((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web OR IP OR (internet ADJ2 protocol)) ADJ3 link) NEAR9 ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/07 12:47 AM
L17	9	((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web OR IP OR (internet ADJ2 protocol)) ADJ3 link) SAME ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/07 12:49 AM
L18	7	((URI OR (uniform ADJ2 resource ADJ2 identifier) OR Web OR IP OR (internet ADJ2 protocol)) ADJ3 link) SAME ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/07 12:50 AM
L19	45	((URI OR (uniform ADJ2 resource ADJ2 identifier) OR Web OR IP OR (internet ADJ2 protocol)) ADJ3 link) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/07 12:53 AM

L20	16	communication)) AND @ad<"20170813" "20140293046"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/07 04:12 PM
L21	7	((URI OR (uniform ADJ2 resource ADJ2 identifier) OR Web OR IP OR (internet ADJ2 protocol)) ADJ3 link) SAME ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/04/22 09:56 PM

PE2E SEARCH - Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
N1	5	((URI OR (uniform ADJ2 resource ADJ2 identifier) OR Web OR IP OR (internet ADJ2 protocol)) ADJ3 link) SAME ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT)	OR	ON	ON	2023/04/22 09:56 PM
N2	5	((URI OR (uniform ADJ2 resource ADJ2 identifier) OR Web OR IP OR (internet ADJ2 protocol)) ADJ3 link) SAME ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT)	OR	ON	ON	2023/04/22 09:56 PM

**CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION
 UNDER 37 CFR 1.102(e)** (Page 1 of 1)

First Named Inventor:	Alexander Dizengof	Nonprovisional Application Number (if known):	17/943,956
Title of Invention:	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently \$0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.
2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.
3. The applicable box is checked below:
 - I. **Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)**
 - i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.
 ---OR---
 - (b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.
 - ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, or the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.
 - II. **Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)**
 - i. A request for continued examination has been filed with, or prior to, this form.
 - ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
 - iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
 - iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
 - v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature	/Cory Smith/	Date	April 17, 2023
Name (Print/Typed)	Cory Smith	Practitioner Registration Number	63,218

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

*Total of 1 forms are submitted.

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	17943956				
Filing Date:	13-Sep-2022				
Title of Invention:	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE				
First Named Inventor/Applicant Name:	Alexander Dizengof				
Filer:	Cory Smith/Lisa Mansur				
Attorney Docket Number:	3010043.2				
Filed as Small Entity					
Filing Fees for Utility under 35 USC 111(a)					
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)	
Basic Filing:					
REQUEST FOR PRIORITIZED EXAMINATION	2817	1	1680	1680	
Pages:					
Claims:					
Miscellaneous-Filing:					
Petition:					
Patent-Appeals-and-Interference:					
Post-Allowance-and-Post-Issuance:					

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
RCE- 1ST REQUEST	2801	1	544	544
Total in USD (\$)				2224

Electronic Acknowledgement Receipt

EFS ID:	47855603
Application Number:	17943956
International Application Number:	
Confirmation Number:	2316
Title of Invention:	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE
First Named Inventor/Applicant Name:	Alexander Dizengof
Customer Number:	46019
Filer:	Cory Smith/Lisa Mansur
Filer Authorized By:	Cory Smith
Attorney Docket Number:	3010043.2
Receipt Date:	17-APR-2023
Filing Date:	13-SEP-2022
Time Stamp:	18:49:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$2224
RAM confirmation Number	E20234GI50179004
Deposit Account	024467
Authorized User	Lisa Mansur

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)
 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	3010043-000002-RCE-Transmittal.pdf	1667173	no	3
			d88fe9076779854af9d7ea383459d09d85a6ff1f		
Warnings:					
Information:					
2		3010043-000002-Response-to-Final-Office-Action.pdf	204517	yes	15
			a154a28edc9ba02cafcc7784f986e59bc9386b21b		
Multipart Description/PDF files in .zip description					
Document Description			Start	End	
Amendment Submitted/Entered with Filing of Continued Prosecution Application (CPA)/Request for Continued Examination(RCE)			1	1	
Claims			2	7	
Applicant Arguments/Remarks Made in an Amendment			8	15	
Warnings:					
Information:					
3	COVID-19 Prioritized Examination Request	3010043-000001-Track-1-Request-for-Prioritized-Examination.pdf	141696	no	2
			31a4e838a9046c6fbd57e4f0d7ca1ab99b059e970		
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	40797	no	2
			4b2cd3c536431a1fb32ea0b659607ad4c039292c		
Warnings:					
Information:					
Total Files Size (in bytes):			2054183		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc code: RCEX

Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (01-22)

Approved for use through 05/31/2024. 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	17/943,956	Filing Date	2022-09-13	Docket Number (if applicable)	3010043.2	Art Unit	2646
First Named Inventor	Alexander Dizengof			Examiner Name	Lafontant, Gary		

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 024467

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 (01-22)

Approved for use through 05/31/2024. 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	Cory Smith/	Date (YYYY-MM-DD)	2023-04-17
Name	Cory Smith	Registration Number	63218

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.

I hereby certify that this correspondence is being filed via
EFS-Web with the United States Patent and Trademark Office
on April 17, 2023

BRYAN CAVE LEIGHTON PAISNER LLP

By: /Lisa Mansur/
Lisa Mansur

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 17/943,956	Filed: September 13, 2022
Applicant: Carbyne Ltd.	Primary Examiner: Lafontant, Gary
Inventor(s): Alexander Dizengof	Art Unit: 2646
Title: System, Method, and Computer- Readable Medium for Streaming Real- Time Data from a User Device	Confirmation No.: 2316

**REQUEST FOR CONTINUED EXAMINATION AND
RESPONSE TO OFFICE ACTION**

Primary Examiner Lafontant:

Applicant submits the present Response to Office Action, which addresses the Final Office Action, mailed March 13, 2023, relating to the above-identified patent application. Applicant also submits herewith a Request for Continued Examination. Please reconsider the patent application in view of the amended claims and remarks presented hereinafter, which are submitted as a full and complete response to the Office Action.

AMENDMENTS TO THE CLAIMS begin on page 2.

REMARKS begin on page 8.

AMENDMENTS TO THE CLAIMS

In accordance with 37 C.F.R. §1.121(c), please amend the claims as indicated in marked-up form below, where additions are underlined, deletions are struck through or boxed in double brackets, and new claims are presented without markings.

1. (Currently Amended) A method implemented via execution of computing instructions configured to run at one or more processors, the method comprising:
 - obtaining a phone number of a mobile device used by a user making an emergency call, wherein the emergency call is conducted with a recipient through a first connection;
 - transmitting a uniform resource locator (URL) link to the mobile device through an electronic message, wherein the electronic message is transmitted through a second connection using the phone number, wherein the second connection is different from the first connection, wherein the electronic message allows the user to click on the URL link to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device, and wherein the URL link is associated with the phone number of the mobile device;
 - receiving the real-time video stream from the mobile device through the WebRTC session; and
 - sending the real-time video stream to the recipient for display on a screen of the recipient, wherein the real-time video stream is received through the WebRTC session while audio content of the emergency call is received through the first connection, and wherein the real-time video stream is associated with a unique identifier for the mobile device.

2. (Original) The method of claim 1, wherein the recipient is at least one of an emergency call center or a dispatch unit.

3. (Original) The method of claim 1, wherein at least one of:
 - the first connection is a voice call over a cellular network;
 - the electronic message is a text message; or

the second connection is a text messaging service.

4. (Original) The method of claim 1, wherein the unique identifier comprises the phone number of the mobile device.

5. (Original) The method of claim 1, wherein the real-time video stream is transmitted from the mobile device to the recipient through a server that is separate from the mobile device and the recipient.

6. (Original) The method of claim 5, wherein the server is a proxy server configured to convert a data format of the real-time video stream.

7. (Original) The method of claim 1, wherein the WebRTC session further transmits at least one of (i) GPS location data of the mobile device for display on the screen of the recipient or (ii) one or more photographs taken on the mobile device for display on the screen of the recipient.

8. (Currently Amended) A system comprising:
- processing circuitry; and
 - a non-transitory computer-readable medium storing computing instructions that, when executed on the processing circuitry, cause the processing circuitry to perform:
 - obtaining a phone number of a mobile device used by a user making an emergency call, wherein the emergency call is conducted with a recipient through a first connection;
 - transmitting a uniform resource locator (URL) link to the mobile device through an electronic message, wherein the electronic message is transmitted through a second connection using the phone number, wherein the second connection is different from the first connection, wherein the electronic message allows the user to click on the URL link to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device, and wherein the URL link is associated with the phone number of the mobile device;
 - receiving the real-time video stream from the mobile device through the WebRTC session; and
 - sending the real-time video stream to the recipient for display on a screen of the recipient, wherein the real-time video stream is received through the WebRTC session while audio content of the emergency call is received through the first connection, and wherein the real-time video stream is associated with a unique identifier for the mobile device.
9. (Original) The system of claim 8, wherein the recipient is at least one of an emergency call center or a dispatch unit.
10. (Original) The system of claim 8, wherein at least one of:
- the first connection is a voice call over a cellular network;
 - the electronic message is a text message; and

the second connection is a text messaging service.

11. (Original) The system of claim 8, wherein the unique identifier comprises the phone number of the mobile device.

12. (Original) The system of claim 8, wherein the real-time video stream is transmitted from the mobile device to the recipient through a server that is separate from the mobile device and the recipient.

13. (Original) The system of claim 12, wherein the server is a proxy server configured to convert a data format of the real-time video stream.

14. (Original) The system of claim 8, wherein the WebRTC session further transmits at least one of (i) GPS location data of the mobile device for display on the screen of the recipient or (ii) one or more photographs taken on the mobile device for display on the screen of the recipient.

15. (Currently Amended) A non-transitory computer-readable medium storing computing instructions that, when executed on processing circuitry, cause the processing circuitry to perform:

obtaining a phone number of a mobile device used by a user making an emergency call, wherein the emergency call is conducted with a recipient through a first connection; transmitting a uniform resource locator (URL) link to the mobile device through an electronic message, wherein the electronic message is transmitted through a second connection using the phone number, wherein the second connection is different from the first connection, wherein the electronic message allows the user to click on the URL link to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device, and wherein the URL link is associated with the phone number of the mobile device; receiving the real-time video stream from the mobile device through the WebRTC session; and sending the real-time video stream to the recipient for display on a screen of the recipient, wherein the real-time video stream is received through the WebRTC session while audio content of the emergency call is received through the first connection, and wherein the real-time video stream is associated with a unique identifier for the mobile device.

16. (Original) The non-transitory computer-readable medium of claim 15, wherein the recipient is at least one of an emergency call center or a dispatch unit.

17. (Original) The non-transitory computer-readable medium of claim 15, wherein at least one of:

the first connection is a voice call over a cellular network;
the electronic message is a text message; or
the second connection is a text messaging service.

18. (Original) The non-transitory computer-readable medium of claim 15, wherein the unique identifier comprises the phone number of the mobile device.

19. (Original) The non-transitory computer-readable medium of claim 15, wherein:
 - the real-time video stream is transmitted from the mobile device to the recipient through a server that is separate from the mobile device and the recipient; and
 - the server is a proxy server configured to convert a data format of the real-time video stream.

20. (Original) The non-transitory computer-readable medium of claim 15, wherein the WebRTC session further transmits at least one of (i) GPS location data of the mobile device for display on the screen of the recipient or (ii) one or more photographs taken on the mobile device for display on the screen of the recipient.

REMARKS

I. Formalities

Claims 1-20 are in the subject patent application. Applicant amends claims 1, 8, and 15. No new matter is added herein by these claim amendments. Specifically, support for the claim amendment “the real-time video stream is received through the WebRTC session while audio content of the emergency call is received through the first connection” in each of claims 1, 8, and 15 is found in at least the following portions of the as-filed Specification:

- “the first DUT receives the real-time data and associates the received data with at least an audio content received over the first connection.” Specification at ¶ 21.
- “when the real-time data is sent to the first DUT 140, the identifier that was included within the link is utilized for associating the real-time data with the at least audio content at the first DUT 140.” Specification at ¶ 39.

II. Examiner Interview Summary

On April 10, 2023, Cory Smith and George Chen (attorneys for Applicant) and Alexander Dizengof (inventor of the subject application, and Founder & Chief Technology Officer of Applicant), conducted a telephonic interview with Primary Examiner Gary Lafontant regarding this Application. During this interview, the invention and amendments to overcome the rejections under 35 U.S.C. § 103 were discussed. Applicant thanks Primary Examiner Lafontant for his time and assistance on this matter.

III. Amended Claims 1-20 Are Allowable in View of 35 U.S.C. § 103

A. Amended Claims 1-20 Are Allowable over Piett and Ni

The Patent Office rejects claims 1-20 under 35 U.S.C. § 103 as being allegedly unpatentable over U.S. Patent Application Publication No. 2016/0337831 to Piett et al. (“Piett”) in view of U.S. Patent Application Publication No. 2014/0293046 to Ni (“Ni”). Applicant respectfully submits that Piett and Ni, whether taken alone or in combination, do not teach or suggest every limitation of amended claims 1-20.

1. Amended Independent Claims 1, 8, and 15 Are Allowable

Amended independent claims 1, 8, and 15 require, in part, “*transmitting a uniform resource locator (URL) link to the mobile device* through an electronic message, wherein the electronic message is transmitted *through a second connection using the phone number*, . . . wherein the electronic message allows the user to click on the URL link to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream *from the mobile device*, and wherein the URL link is *associated with the phone number* of the mobile device; receiving the real-time video stream *from the mobile device* through the WebRTC session; . . . wherein *the real-time video stream is received through the WebRTC session while audio content of the emergency call is received through the first connection*; and wherein *the real-time video stream is associated with a unique identifier for the mobile device*” (emphasis added).

Piett does not teach or suggest these limitations. The Patent Office cites to Piett for teaching the pre-amended limitations, but those citations are inapposite, for the reasons explained as follows:

For the limitation “transmitting a uniform resource locator (URL) link to the mobile device through an electronic message,” the Patent Office cites to FIG. 1 (102) and paragraphs 22 and 62-65 of Piett, and asserts “mobile device received URI message to initiate transmission of data through network 106, URI comprises URL.” Office Action at 4. However, paragraph 62 of Piett teaches that the URI is “a SIP From-URI,” which is the “Uniform Resource Identifier” data in the Session Initiation Protocol (SIP). This URI is not a “uniform resource locator (URL) link,” as required by amended independent claims 1, 8, and 15. Moreover, nowhere does Piett teach or suggest “transmitting a uniform resource locator (URL) link *to the mobile device* through an electronic message” (emphasis added), as required by amended independent claims 1, 8, and 15.

For the limitation “the electronic message is transmitted through a second connection using the phone number,” the Patent Office cites to FIG. 1 (106) and paragraphs 22, 39, 42-43, and 60-62 of Piett, and asserts “OTSL communicate with calling device via network 106.” Office Action at 4. However, paragraphs 43, 60-62 of Piett teach public safety access point (PSAP) 108 querying OTSL computing device 110 using a unique device ID in the between OTSL computing device 110 and calling device 102 through network 106. Packet-based communication network 106 cannot be the second connection, as “the electronic message is transmitted through a second

connection *using the phone number*” (emphasis added), per amended independent claims 1, 8, and 15, but Piett does not teach or suggest using *a phone number* in the communications between OTSL 110 and device 102 in packet-based communication network 106.

Nowhere does Piett teach or suggest “*transmitting a uniform resource locator (URL) link to the mobile device* through an electronic message, wherein the electronic message is transmitted *through a second connection using the phone number*, . . . wherein the electronic message allows the user to click on the URL link to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream *from the mobile device*, and wherein the URL link is *associated with the phone number* of the mobile device; receiving the real-time video stream *from the mobile device* through the WebRTC session; . . . wherein *the real-time video stream is received through the WebRTC session while audio content of the emergency call is received through the first connection*; and wherein *the real-time video stream is associated with a unique identifier for the mobile device*” (emphasis added), as required by amended independent claims 1, 8, and 15.

Meanwhile, Ni does not provide the missing teachings of Piett, whether taken alone or in combination. The Patent Office cites to Ni for teaching the pre-amended limitations, but those citations are inapposite, for the reasons explained as follows:

For the limitation “the electronic message allows the user to click on the URL link to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device,” the Patent Office cites to paragraphs 16, 31, and 44 of Ni, and asserts “creating a streaming video session between two communication devices in a network using WebRTC session protocol providing hyperlink to the streaming device.” Office Action at 5. However, Ni teaches:

Security control system 120 may implement security services, including surveillance, alarm, response and deterrence functions, etc., for surveillance premises 110 using a web based system, such as Web real time communication (webRTC), a technology standard defined by the World Wide Web Consortium (W3C). WebRTC may enable browser to browser applications, such as video chat, voice calling, and peer to peer (P2P) file sharing that may be used to implement security functions associated with security control system 120 as described herein with respect to FIG. 4.

Ni at ¶ 16. Ni also teaches, “Security control device 302 may monitor continuous feeds from multiple cameras 320 or may sample multiple video feeds, based on CSS 322.” Ni at ¶ 31. Ni additionally teaches, “Cameras 320 may be stationary cameras or may include associated servomotors that allow a degree of motion in viewing an area under surveillance.” Ni at ¶ 34. Ni further teaches:

Alert module 430 may provide an alert to a predetermined group of devices in response to detection of a triggering event (i.e., unauthorized access to surveillance premises 110). The alert may be sent via email, short message, social network and/or other types of online application notifications to the user and any specified members authorized by the user (e.g., family members, friends, designated security management company or police/fire/emergency departments, etc.) to receive such notifications. The notification may contain a short event description, a recommended action and a link to receive the webRTC call initiated by alert module 430. Additionally, or alternatively, alert module 430 may convert and/or transcode signals (e.g., still image and/or video signals) from cameras 320 and additional sensors to enable presentation in web browsers of user devices 170.

Ni at ¶ 44.

In other words, Ni teaches sending video data from cameras 320 stationed in a home to be displayed on mobile user devices 170 using WebRTC, not transmitting a real-time video stream from the mobile device. Ni does not teach “the electronic message allows the user to click on the URL link to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream *from the mobile device*” (emphasis added), as required by amended independent claims 1, 8, and 15.

For the limitation “the URL link is associated with the phone number of the mobile device,” the Patent Office cites to paragraphs 18, 50, and 76 of Ni, and asserts “identifying a user account.” Office Action at 5. However, a user account is not a phone number. Ni does not teach using a phone number, let alone “the URL link is *associated with the phone number* of the mobile device” (emphasis added), as required by amended independent claims 1, 8, and 15.

For the limitation “receiving the real-time video stream from the mobile device through the WebRTC session,” the Patent Office cites to paragraphs 44, 47, and 77 of Ni, and asserts “real time video data streaming.” Office Action at 6. However, as explained above, Ni does not teach using a phone number. Moreover, Ni does not teach “receiving the real-time video stream *from the*

mobile device through the WebRTC session” (emphasis added), as required by amended independent claims 1, 8, and 15.

For the limitation “the real-time video stream is associated with a unique identifier for the mobile device,” the Patent Office cites to paragraphs 47 and 76-77 of Ni, and asserts “WebRTC associate identifier with different dedicatedUE.” Office Action at 6. However, Ni teaches:

As further shown in FIG. 9, process 900 may include identifying a user account associated with the web call (block 920). For example, web server 130 may receive a user account identifier from security control device 302.

At block 930, web server 130 may determine a user preference for alerts. For example, web server 130 may search a database that includes user preferences for sending alerts. The preferences may include persons, devices, and online accounts that the user has preselected to receive alerts.

Ni at ¶¶ 76-77. In other words, Ni teaches using a user account, not a unique identifier for the mobile device. Ni does not teach “the real-time video stream is associated with a unique identifier for the mobile device,” as required by amended independent claims 1, 8, and 15.

Moreover, with respect to the newly added limitation, “the real-time video stream is received through the WebRTC session while audio content of the emergency call is received through the first connection,” Ni teaches establishing an Internet-based WebRTC audio/video call. Ni at ¶¶ 16, 49-50. However, Ni, does not teach that the WebRTC call can occur while the separate emergency call is occurring over the first connection. Ni does not teach “the real-time video stream is received through the WebRTC session while audio content of the emergency call is received through the first connection,” as required by amended independent claims 1, 8, and 15.

Nowhere does Ni teach or suggest “***transmitting a uniform resource locator (URL) link to the mobile device*** through an electronic message, wherein the electronic message is transmitted ***through a second connection using the phone number***, . . . wherein the electronic message allows the user to click on the URL link to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream ***from the mobile device***, and wherein the URL link is ***associated with the phone number*** of the mobile device; receiving the real-time video stream ***from the mobile device*** through the WebRTC session; . . . wherein ***the real-time video stream is received through the WebRTC session while audio content of the emergency call is received through the first connection***; and wherein ***the real-time video stream is associated with a unique***

identifier for the mobile device” (emphasis added), as required by amended independent claims 1, 8, and 15. Accordingly, Ni does nothing to rectify the deficiencies of Piett, whether taken alone or in combination.

Accordingly, Applicant respectfully requests the allowance of amended independent claims 1, 8, and 15.

2. Dependent Claims 2-7, 9-14, and 16-20 Are Allowable

Applicant overcomes the rejection of claims 2-7, 9-14, and 16-20 under 35 U.S.C. § 103 as being allegedly unpatentable over Piett and Ni because claims 2-7, 9-14, and 16-20 depend, directly or indirectly, from amended independent claims 1, 8, or 15. Dependent claims must be construed to include all of the limitations of the claims from which they depend, as required by 37 C.F.R. § 1.75(c) and MPEP § 608.01(n). The deficiencies of Piett and Ni in relation to amended independent claims 1, 8, and 15 are discussed above. Accordingly, the Patent Office should allow dependent claims 2-7, 9-14, and 16-20 for at least the same reasons as listed earlier for amended independent claims 1, 8, and 15, as well as for their own respective limitations.

For example, claims 3, 10, and 17 are not taught by Piett or Ni, whether taken alone or in combination. The Patent Office cites to paragraph 38 of Piett, Office Action at 7, but paragraph 38 of Piett teaches: “It should be appreciated that other types of emergency communications (e.g., text messages) can be transmitted via the *cellular communications network 104* as described herein” (emphasis added). However, claim 1 recites “the electronic message is transmitted through a second connection using the phone number,” and the Patent Office has asserted the second connection is network 106, not cellular communications network 104. Office Action at 4, so any communications through network 104 (not network 106) in Piett cannot be related to the electronic message. Accordingly, Piett does not teach or suggest “the electronic message is a text message,” as required by claims 3, 10, and 17.

As a further example, claims 7, 14, and 20 are not taught by Piett or Ni, whether taken alone or in combination. The Patent Office cites to paragraphs 25, 43, and 60 of Piett, which teach an app pushing location data, not a WebRTC session transmitting GPS location data. Nowhere do Piett or Ni teach or suggest “the WebRTC session further transmits at least one of (i) GPS location data of the mobile device for display on the screen of the recipient or (ii) one or more photographs

taken on the mobile device for display on the screen of the recipient,” as required by claims 7, 14, and 20.

CONCLUSION

Applicant has made an earnest attempt to place this case in condition for allowance. In light of the amended claims and remarks set forth above, Applicant respectfully requests consideration and allowance of all of the pending claims.

As Applicant's remarks with respect to the Patent Office's rejections are sufficient to overcome these rejections, Applicant's silence as to certain assertions or requirements applicable to such rejections (e.g., whether a reference constitutes prior art, whether a reference shows, discloses, teaches, or suggests a claim limitation, whether a reference is non-analogous art, motivation to combine references, etc.) is not a concession by Applicant that such assertions are accurate or such requirements have been met, and Applicant reserves the right to analyze and dispute the same in the future. Also, Applicant asserts that no one should construe any contents of this paper as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment or cancellation of any claim does not necessarily signify a concession of unpatentability of the claim prior to its amendment.

Applicant believes \$2,224.00 in fees are due (\$544.00 under 37 C.F.R. § 1.114 and 37 C.F.R. § 1.17(e)(1) in connection with filing this first Request for Continued Examination, and \$1,680.00 for a request for prioritized examination), to be charged to Account No. 02-4467. However, the Commissioner for Patents is hereby authorized to charge any additional fees necessitated by the filing of this paper, or credit any overpayment, to Account No. 02-4467.

If matters can be discussed by telephone to further the prosecution of this application, Applicant invites the Examiner to call the undersigned attorney at the Examiner's convenience.

Respectfully submitted,

By: /Cory G. Smith/

BRYAN CAVE LEIGHTON PAISNER LLP
Two North Central Avenue
Suite 2100
Phoenix, AZ 85004-4406

Cory G. Smith
Attorney for Applicant
Reg. No. 63,218
Tel. (602) 364-7442

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875		Application or Docket Number 17/943,956		Filing Date 09/13/2022	<input type="checkbox"/> To be Mailed	
ENTITY: <input type="checkbox"/> LARGE <input checked="" type="checkbox"/> SMALL <input type="checkbox"/> MICRO						
APPLICATION AS FILED - PART I						
	(Column 1)	(Column 2)				
FOR	NUMBER FILED	NUMBER EXTRA		RATE (\$)	FEE (\$)	
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A		
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A		N/A		
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A		
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	* 0		x \$50 =	0	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	* 0		x \$240 =	0	
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))						
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	0	
APPLICATION AS AMENDED - PART II						
	(Column 1)	(Column 2)	(Column 3)			
AMENDMENT	04/17/2023	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 20	Minus ** 20	= 0	x \$40 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus *** 3	= 0	x \$192 =	0
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))					
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	x \$0 =	
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x \$0 =	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))					
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.					LIE	
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".					/GERALDINE L STANLEY/	
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".						
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.						

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, 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.



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
Row 1: 17/943,956, 09/13/2022, Alexander Dizengof, 3010043.2, 2316
Row 2: 46019, 7590, 04/14/2023, BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX), TWO NORTH CENTRAL AVENUE, SUITE 2100, PHOENIX, AZ 85004
Row 3: EXAMINER LAFONTANT, GARY
Row 4: ART UNIT 2646, PAPER NUMBER
Row 5: NOTIFICATION DATE 04/14/2023, DELIVERY MODE ELECTRONIC

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

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

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

PXBCIPDocketing@bcplaw.com

<i>Applicant-Initiated Interview Summary</i>	Application No. 17/943,956	Applicant(s) Dizengof, Alexander		
	Examiner GARY LAFONTANT	Art Unit 2646	AIA (First Inventor to File) Status Yes	Page 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	Title	Type
GARY LAFONTANT	Primary Examiner	Telephonic
Cory Smith	Attorney	
George Chen	Attorney	
Alex Dizengof	Attorney	

Date of Interview: 10 April 2023

Issues Discussed:

35 U.S.C. 103

Applicant discusses about the current rejection being improper because according to the invention, there are two channels of communication being operated simultaneously, the first audio call and the WebRTC video feed after the user click on the receiving link and the references used for the rejection do not teach these limitations. Examiner argues that the claim as written does not teach about these separated communication link and that if described in amended claims would overcome current references. Applicant took account of Examiner suggestion and will proceed accordingly but no agreement was reached in term of allowance.

/GARY LAFONTANT/ Examiner, Art Unit 2646	
<p>Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04</p> <p>Please further see: MPEP 713.04 Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b) 37 CFR § 1.2 Business to be transacted in writing</p>	

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

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
Row 1: 17/943,956, 09/13/2022, Alexander Dizengof, 3010043.2, 2316
Row 2: 46019, 7590, 03/13/2023, BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX), TWO NORTH CENTRAL AVENUE, SUITE 2100, PHOENIX, AZ 85004
Row 3: EXAMINER LAFONTANT, GARY
Row 4: ART UNIT 2646, PAPER NUMBER
Row 5: NOTIFICATION DATE 03/13/2023, DELIVERY MODE ELECTRONIC

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

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

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

PXBCIPDocketing@bcplaw.com

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

The amendment filed on has been acknowledged.

Amendment Summary

Claims 1, 8, 15 are amended.

Response to Arguments/Amendment

Applicant's arguments with respect to **claims #1-20** have been considered but are **moot** because the arguments do not apply to the **combination** of the references being used for the **current rejection** of the above claim.

Claim Rejections - 35 USC § 103

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

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the

claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim(s) 1-20 are rejected under **35 U.S.C. 103** as being unpatentable over **Piett (US 2016/0337831 A1)** in view of **Ni (US 2014/0293046 A1)**

Regarding Claims 1, 8, 15

Piett discloses a method implemented via execution of computing instructions **(See {0016}; [0040]; instructions to perform method)** configured to run at one or more processors **(Fig.1(108)(Fig.1(110)))**,

the method comprising:

obtaining a phone number **(See [0043]; [0060-0062]; obtaining at least one of the unique identifier including MSID)** of a mobile device **(Fig.1(102))** used by a user **(See [0043]; a user initiating communication)** making an emergency call **(See [0043]; during emergency call);**

wherein the emergency call is conducted with a recipient **(Fig.1(108))** through a first connection **(See [0043]; emergency through cellular communications to PSAP recipient);**

transmitting a uniform resource locator (URI) to the mobile device (**Fig.1(102)**) through an electronic message (**See [0022]; [0062-0065]; mobile device received URI message to initiate transmission of data through network 106**),

wherein the electronic message (**See [0022]; initiation message is transmitted to calling device to start transmission**) is transmitted through a second connection (**See Fig.1(106); [0022]; [0039]; [0042-0043]; OTSL communicate with calling device via network 106**) using the phone number (**See [0043]; [0060-0062]; obtaining at least one of the unique identifier including Message ID**),

wherein the second connection is different from the first connection (**See Fig.1; cellular network 104 different than packet network 106**),

wherein a URI is associated with the phone number of the mobile device (**See [0062-0065]**).

But **Piett** fails to explicitly recite

wherein the electronic message allows the user ***to click on the URL link to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time***

Communication) session to transmit real-time video stream from the mobile device, and

wherein the URL link is associated with the phone number of the mobile device ;

receiving the real-time video stream from the mobile device through the WebRTC session; and

sending the real-time video stream to the recipient for display on a screen of the recipient,

wherein the real-time video stream is associated with a unique identifier for the mobile device.

However in analogous art,

Ni teaches about creating a streaming video session between two communication devices in a network using WebRTC session protocol providing hyperlink to the streaming device (See [0016]; [0031]; [0044]; hyperlink is provided to other device in a network to start streaming video);

wherein the URL link is associated with an identification of the mobile device (See [0018]; [0050]; [0076]; identifying a user account);

receiving the real-time video stream from the mobile device through the WebRTC session (**See [0044]; [0047]; [0077]; real time video data streaming**); and

sending the real-time video stream to the recipient for display on a screen of the recipient (**See [0044]; [0047]; [0050]; end user display of video using web browser**),

wherein the real-time video stream is associated with a unique identifier for the mobile device (**See [0044]; [0076-0077]; WebRTC associate identifier with different dedicatedUE**) .

Piett and Ni are analogous art because they all pertain to streaming data using network communication channel between two communication devices using different communication protocol. **Piett** teaches about setting up an emergency call through a calling device to a PSAP. The latter then requesting a location data of the calling device. **Ni** teaches about setting up WebRTC between users though web link using device identities to stream audio and video data. **Piett** could use **Ni** features (WebRTC) to stream video data of caller with specific ID experiencing emergency situation. Therefore it would have been obvious at the time of the filing of the application for one of ordinary skill to combine **Piett** and **Ni** as to obtain an efficient emergency rescue communication system.

Regarding Claim 2, 9, 16

Piatt and Ni teach all the features with respect to **claim 1, 8, 15 and Piatt** further teaches

wherein the recipient is at least one of
an emergency call center (**Fig,1(108); PSAP/dispatch**)
or
a dispatch unit (**See [0013]; [0040]; PSAP/dispatch**).

Regarding Claim 3, 10, 17

Piatt and NI teach all the features with respect to **claim 1, 8, 15 and Piatt** further teaches

wherein at least one of:

the first connection is a voice call over a cellular network (**See [0036-0037];
emergency call over GSM type cellular**);

the electronic message is a text message (**See [0038]; emergency text**); or

the second connection is a text messaging service (**See [0086]; text message to caller**).

Regarding Claim 4, 11, 18

Piett and Ni teach all the features with respect to **claim 1, 8, 15 and Piett** further teaches

wherein the unique identifier comprises the phone number of the mobile device (**See [0043]; [0047]; [0060-0062]; phone number retrieved from transmission message**) .

Regarding Claim 5, 12, 19

Piett and Ni teach all the features with respect to **claim 1, 8, 15 and Ni** further teaches

wherein the real-time video stream (**See [0044]; [0076-0077]**) is transmitted from the mobile device (**Fig.1(120)**) to the recipient (**Fig.1(15)(160)(170)**) through a server (**Fig.1(130)**) that is separate from the mobile device and the recipient (**See Fig.1; [0014]**) .

Regarding Claim 6, 13, 20

Piett and Ni teach all the features with respect to **claim 5, 12, 15 and NI** further teaches

wherein the server is a proxy server (**See Fig.1(130)(135);[0014]; [0017-0018]]**) configured to convert a data format of the real-time video stream (**See [0044]; select format on how to present data through the network**).

Regarding Claim 7, 14

Piett and Ni teach all the features with respect to **claim 1, 8 and Piett** further teaches

wherein the session further transmits at least one of

(i) GPS location data of the mobile device for display on the screen of the recipient (**See [0025]; [0043]; [0060]; location data is provided to be displayed**) or

(ii) one or more photographs taken on the mobile device for display on the screen of the recipient.

(The term “ at least one” translate to the satisfaction of one or more of the limitation can be analyzed)

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to GARY LAFONTANT whose telephone number is (571)272-3037. The examiner can normally be reached 9:00AM -5:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lester Kincaid can be reached on 571-272-7922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent-center> for more information about Patent Center and <https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/GARY LAFONTANT/

Examiner, Art Unit 2646

Notice of References Cited	Application/Control No. 17/943,956	Applicant(s)/Patent Under Reexamination Dizengof, Alexander	
	Examiner GARY LAFONTANT	Art Unit 2646	Page 1 of 1

U.S. PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A US-20140293046-A1	10-2014	Ni; James J.	H04N7/181	348/143
B					
C					
D					
E					
F					
G					
H					
I					
J					
K					
L					
M					


FOREIGN PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
N					
O					
P					
Q					
R					
S					
T					

NON-PATENT DOCUMENTS

*	U	V	W	X
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)			

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<i>Search Notes</i> 	Application/Control No. 17/943,956	Applicant(s)/Patent Under Reexamination Dizengof, Alexander
	Examiner GARY LAFONTANT	Art Unit 2646

CPC - Searched*		
Symbol	Date	Examiner
All	11/18/2022	GL
ALL	03/08/2023	GL

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Pe2E SEArch	11/18/2022	GL
PE2E Search	03/08/2023	GL

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/GARY LAFONTANT/ Examiner, Art Unit 2646	
---	--

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	9420116		2016-08-16	Hamilton et al.		
	2	9167379		2015-10-20	Hamilton et al.		
	3	8976939		2015-03-10	Hamilton et al.		
	4	8270935		2012-09-18	Lee		
	5	8145183		2012-03-27	Barbeau et al.		
	6	7751826		2010-07-06	Gardner et al.		
If you wish to add additional U.S. Patent citation information please click the Add button.							Add
U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17943956
	Filing Date		2022-09-13
	First Named Inventor	Alexander Dizengof	
	Art Unit		2646
	Examiner Name	Lafontant, Gary	
	Attorney Docket Number		3010043.2

1	20140007158		2014-01-02	Bhagwat
2	20120202447		2012-08-09	Edge et al.
3	20120190384		2012-07-26	Marr et al.
4	20120149324		2012-06-14	Daly
5	20120027189		2012-02-02	Shaffer et al.
6	20110111726		2011-05-12	Kholaif et al.
7	20110086607		2011-04-14	Wang et al.
8	20100261492		2010-10-14	Salafia et al.
9	20100220840		2010-09-02	Ray et al.
10	20100174560		2010-07-08	Quan et al.
11	20050176441		2005-08-11	Jurecka

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17943956	
	Filing Date		2022-09-13	
	First Named Inventor	Alexander Dizengof		
	Art Unit	2646		
	Examiner Name	Lafontant, Gary		
	Attorney Docket Number	3010043.2		

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ^{2]}	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button.

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	PCT International Search Report and Written Opinion issued in corresponding PCT Application No. PCT/JS2014/051952, mailed November 24, 2014.	

If you wish to add additional non-patent literature document citation information please click the Add button.

EXAMINER SIGNATURE

Examiner Signature	<u>/GARY LAFONTANT/</u>	Date Considered	03/08/2023
--------------------	-------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Cory Smith/	Date (YYYY-MM-DD)	2022-12-13
Name/Print	Cory Smith	Registration Number	63218

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour 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. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

U.S. PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S. PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	
	1	20150056946	A1	2015-02-26	Leggett et al.		

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2014182638	WO	A2	2014-11-13	Decharms		

If you wish to add additional Foreign Patent Document citation information please click the Add button. Add

NON-PATENT LITERATURE DOCUMENTS								Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.						T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17943956
	Filing Date		2022-09-13
	First Named Inventor	Alexander Dizengof	
	Art Unit	2646	
	Examiner Name	Lafontant, Gary	
	Attorney Docket Number	3010043.2	

1		"Notice of Opposition of a European Patent," filed in EP Patent No. 3,445,016, by Dentons UK and Middle East LLP, dated December 9, 2022.
---	--	---

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/GARY LAFONTANT/	Date Considered	03/08/2023
--------------------	------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- See attached certification statement.
- The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Cory Smith/	Date (YYYY-MM-DD)	2023-02-23
Name/Print	Cory Smith	Registration Number	63218

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour 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. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

U.S. PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S. PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20170034353		2017-02-02	Bell et al.	

	2	20160037126		2016-02-04	Polyakov et al.	
--	---	-------------	--	------------	-----------------	--

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2014158562	WO		2014-10-02	Echostar Technologies LLC		

If you wish to add additional Foreign Patent Document citation information please click the Add button.

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17943956
	Filing Date		2022-09-13
	First Named Inventor	Alexander Dizengof	
	Art Unit	2646	
	Examiner Name	Lafontant, Gary	
	Attorney Docket Number	3010043.2	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	LAND MOBILE, Wireless Communications for Business, www.landmobile.com, October 2016.	
	2	TV News Central, "New App to Allow 999 Callers to Live Stream from the Scene of Emergencies," dated 22 October 2014, (downloaded 14 November 2022).	
	3	Directors Club NEWS, "Capita and West Midlands Fire Service Launch 999EYE," dated 7 November 2016, (downloaded 14 November 2022).	
	4	British APCO Conference, https://www.mobilemark.com/bapco-annual-conference-exhibition/, (downloaded 17 November 2022).	
	5	PageOne Website, https://www.pageone.co.uk/999eye-wins-bapco-innovation-award/, (downloaded 14 November 2022).	
	6	YouTube Video, "Two Years of 999eye," https://www.youtube.com/watch?v=8E-DVij0km8, dated 15 November 2018, (viewed 21 November 2022).	

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/GARY LAFONTANT/	Date Considered	03/08/2023
--------------------	------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17943956
	Filing Date		2022-09-13
	First Named Inventor	Alexander Dizengof	
	Art Unit	2646	
	Examiner Name	Lafontant, Gary	
	Attorney Docket Number	3010043.2	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Cory Smith/	Date (YYYY-MM-DD)	2023-01-06
Name/Print	Cory Smith	Registration Number	63218

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour 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. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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.

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	10686618		2020-06-16	Dizengof		
	2	9792654		2017-10-17	Limas et al.		
	3	9414225		2016-08-09	Timariu et al.		
	4	9301117		2016-03-29	Leggett et al.		
	5	8504090		2013-08-06	Klein et al.		
If you wish to add additional U.S. Patent citation information please click the Add button.							Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	20200313922		2020-10-01	Dizengof		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17943956
	Filing Date		2022-09-13
	First Named Inventor	Alexander Dizengof	
	Art Unit	2646	
	Examiner Name	Lafontant, Gary	
	Attorney Docket Number	3010043.2	

2	20190052474		2019-02-14	Dizengof
3	20170180964		2017-06-22	Mehta et al.
4	20170164175		2017-06-08	Bozik et al.
5	20170126751		2017-05-04	Stach et al.
6	20170124853		2017-05-04	Mehta et al.
7	20160381091		2016-12-29	O'Connor et al.
8	20160088455		2016-03-24	Bozik et al.
9	20160014585		2016-01-14	Sundararaj et al.
10	20150099482		2015-04-09	Schmitz
11	20150056946		2015-02-26	Leggett et al.
12	20070028279		2007-02-01	Kim

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		17943956	
	Filing Date		2022-09-13	
	First Named Inventor	Alexander Dizengof		
	Art Unit	2646		
	Examiner Name	Lafontant, Gary		
	Attorney Docket Number	3010043.2		

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ^{2]}	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2992692	EU		2016-03-09	Decharms		

If you wish to add additional Foreign Patent Document citation information please click the Add button.

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	European Search Report and the European Search Opinion Dated 08 April 2022 from the European Patent Office Re. Application No. 22152510.8, (11 Pages).	
	2	European Search Report and the European Search Opinion Dated 06 December 2018 from the European Patent Office Re. Application No. 18188748.0, (10 Pages).	

If you wish to add additional non-patent literature document citation information please click the Add button.

EXAMINER SIGNATURE

Examiner Signature	<u>/GARY LAFONTANT/</u>	Date Considered	03/08/2023
--------------------	-------------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Cory Smith/	Date (YYYY-MM-DD)	2022-12-13
Name/Print	Cory Smith	Registration Number	63218

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour 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. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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.

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	8	"20150106528"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/11/18 04:21 PM
L2	2	"20150106528"	(US-PGPUB; USPAT)	OR	ON	ON	2022/11/18 04:21 PM
L3	2	"20160337831"	(US-PGPUB; USPAT)	OR	ON	ON	2022/11/18 04:22 PM
L4	0	(URL ADJ2 link) NEAR9 WebRTC AND @ad<"20170813"	(DERWENT)	OR	ON	ON	2023/02/28 06:05 PM
L5	2	(URL ADJ2 link) NEAR9 WebRTC AND @ad<"20170813"	(USPAT)	OR	ON	ON	2023/02/28 06:05 PM
L6	1	((URL OR (uniform ADJ2 resource ADJ2 locator)) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(DERWENT)	OR	ON	ON	2023/03/01 12:46 AM
L7	1	((URL OR (uniform ADJ2 resource ADJ2 locator)) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) SAME2 (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(DERWENT)	OR	ON	ON	2023/03/01 12:47 AM
L8	3	((URL OR (uniform ADJ2 resource ADJ2 locator)) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) SAME2 (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 12:47 AM
L9	5	((URL OR (uniform ADJ2 resource ADJ2	(US-PGPUB; USPAT; USOCR; FIT (AU, AP,	OR	ON	ON	2023/03/01 01:11 AM

L10	20	locator)) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) AND (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 01:14 AM
L11	1265	((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 01:32 AM
L12	6	((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) AND (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 01:33 AM
L13	6	((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web OR IP OR (internet ADJ2 protocol)) ADJ2 link) NEAR9 ((phone OR telephone) NEAR2 number) AND (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 12:41 PM
L14	562	((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web OR IP OR (internet ADJ2 protocol))) NEAR9 ((phone OR telephone) NEAR2 number) AND (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication))	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 12:41 PM

L15	107	AND @ad<"20170813" ((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web OR IP OR (internet ADJ2 protocol))) NEAR9 ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/01 12:42 PM
L16	3	((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web OR IP OR (internet ADJ2 protocol)) ADJ3 link) NEAR9 ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/07 12:47 AM
L17	9	((URL OR (uniform ADJ2 resource ADJ2 locator) OR Web OR IP OR (internet ADJ2 protocol)) ADJ3 link) SAME ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/07 12:49 AM
L18	7	((URI OR (uniform ADJ2 resource ADJ2 identifier) OR Web OR IP OR (internet ADJ2 protocol)) ADJ3 link) SAME ((phone OR telephone) NEAR2 number) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/07 12:50 AM
L19	45	((URI OR (uniform ADJ2 resource ADJ2 identifier) OR Web OR IP OR (internet ADJ2 protocol)) ADJ3 link) SAME (WebRTC OR (Web ADJ2 Real ADJ2 Time ADJ2 communication)) AND @ad<"20170813"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/07 12:53 AM

L20	16	communication)) AND @ad<"20170813" "20140293046"	(US-PGPUB; USPAT; USOCR; FIT (AP, AT, AU, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2023/03/07 04:12 PM
-----	----	---	---	----	----	----	------------------------

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

I hereby certify that this correspondence is being filed via
EFS-Web with the United States Patent and Trademark Office
on February 24, 2023

BRYAN CAVE LEIGHTON PAISNER LLP

By: /Lisa Mansur/
Lisa Mansur

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 17/943,956	Filed: September 13, 2022
Applicant: Carbyne Ltd.	Primary Examiner: Lafontant, Gary
Inventor(s): Alexander Dizengof	Art Unit: 2646
Title: System, Method, and Computer- Readable Medium for Streaming Real- Time Data from a User Device	Confirmation No.: 2316

RESPONSE TO OFFICE ACTION

Primary Examiner Lafontant:

This response addresses the non-final Office Action, mailed November 25, 2022, relating to the above-identified application. Please reconsider the patent application in view of the amendments to the claims and the remarks presented hereinafter, which are submitted as a full and complete response to the Office Action.

AMENDMENTS TO THE CLAIMS begin on page 2.

REMARKS begin on page 8.

AMENDMENTS TO THE CLAIMS

In accordance with 37 C.F.R. §1.121(c), please amend the claims as indicated in marked-up form below, where additions are underlined, deletions are struck through or boxed in double brackets, and new claims are presented without markings.

1. (Currently Amended) A method implemented via execution of computing instructions configured to run at one or more processors, the method comprising:
 - obtaining a phone number of a mobile device used by a user making an emergency call, wherein the emergency call is conducted with a recipient through a first connection;
 - transmitting a uniform resource locator (URL) link to the mobile device through an electronic message, wherein the electronic message is transmitted through a second connection using the phone number, wherein the second connection is different from the first connection, wherein the electronic message allows the user to click on the URL link to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device, and wherein the URL link is associated with the phone number of the mobile device;
 - receiving the real-time video stream from the mobile device through the WebRTC session; and
 - sending the real-time video stream to the recipient for display on a screen of the recipient, wherein the real-time video stream is associated with a unique identifier for the mobile device.

2. (Original) The method of claim 1, wherein the recipient is at least one of an emergency call center or a dispatch unit.

3. (Original) The method of claim 1, wherein at least one of:
 - the first connection is a voice call over a cellular network;
 - the electronic message is a text message; or
 - the second connection is a text messaging service.

4. (Original) The method of claim 1, wherein the unique identifier comprises the phone number of the mobile device.
5. (Original) The method of claim 1, wherein the real-time video stream is transmitted from the mobile device to the recipient through a server that is separate from the mobile device and the recipient.
6. (Original) The method of claim 5, wherein the server is a proxy server configured to convert a data format of the real-time video stream.
7. (Original) The method of claim 1, wherein the WebRTC session further transmits at least one of (i) GPS location data of the mobile device for display on the screen of the recipient or (ii) one or more photographs taken on the mobile device for display on the screen of the recipient.

8. (Currently Amended) A system comprising:
- processing circuitry; and
 - a non-transitory computer-readable medium storing computing instructions that, when executed on the processing circuitry, cause the processing circuitry to perform:
 - obtaining a phone number of a mobile device used by a user making an emergency call, wherein the emergency call is conducted with a recipient through a first connection;
 - transmitting a uniform resource locator (URL) link to the mobile device through an electronic message, wherein the electronic message is transmitted through a second connection using the phone number, wherein the second connection is different from the first connection, wherein the electronic message allows the user to click on the URL link to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device, and wherein the URL link is associated with the phone number of the mobile device;
 - receiving the real-time video stream from the mobile device through the WebRTC session; and
 - sending the real-time video stream to the recipient for display on a screen of the recipient, wherein the real-time video stream is associated with a unique identifier for the mobile device.
9. (Original) The system of claim 8, wherein the recipient is at least one of an emergency call center or a dispatch unit.
10. (Original) The system of claim 8, wherein at least one of:
- the first connection is a voice call over a cellular network;
 - the electronic message is a text message; and
 - the second connection is a text messaging service.

11. (Original) The system of claim 8, wherein the unique identifier comprises the phone number of the mobile device.
12. (Original) The system of claim 8, wherein the real-time video stream is transmitted from the mobile device to the recipient through a server that is separate from the mobile device and the recipient.
13. (Original) The system of claim 12, wherein the server is a proxy server configured to convert a data format of the real-time video stream.
14. (Original) The system of claim 8, wherein the WebRTC session further transmits at least one of (i) GPS location data of the mobile device for display on the screen of the recipient or (ii) one or more photographs taken on the mobile device for display on the screen of the recipient.

15. (Currently Amended) A non-transitory computer-readable medium storing computing instructions that, when executed on processing circuitry, cause the processing circuitry to perform:

obtaining a phone number of a mobile device used by a user making an emergency call, wherein the emergency call is conducted with a recipient through a first connection; transmitting a uniform resource locator (URL) link to the mobile device through an electronic message, wherein the electronic message is transmitted through a second connection using the phone number, wherein the second connection is different from the first connection, wherein the electronic message allows the user to click on the URL link to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device, and wherein the URL link is associated with the phone number of the mobile device; receiving the real-time video stream from the mobile device through the WebRTC session; and sending the real-time video stream to the recipient for display on a screen of the recipient, wherein the real-time video stream is associated with a unique identifier for the mobile device.

16. (Original) The non-transitory computer-readable medium of claim 15, wherein the recipient is at least one of an emergency call center or a dispatch unit.

17. (Original) The non-transitory computer-readable medium of claim 15, wherein at least one of:

the first connection is a voice call over a cellular network;
the electronic message is a text message; or
the second connection is a text messaging service.

18. (Original) The non-transitory computer-readable medium of claim 15, wherein the unique identifier comprises the phone number of the mobile device.

19. (Original) The non-transitory computer-readable medium of claim 15, wherein:
the real-time video stream is transmitted from the mobile device to the recipient through a server that is separate from the mobile device and the recipient; and
the server is a proxy server configured to convert a data format of the real-time video stream.
20. (Original) The non-transitory computer-readable medium of claim 15, wherein the WebRTC session further transmits at least one of (i) GPS location data of the mobile device for display on the screen of the recipient or (ii) one or more photographs taken on the mobile device for display on the screen of the recipient.

REMARKS

I. Formalities

Claims 1-20 are in the subject patent application. Applicant amends claims 1, 8, and 15. No new matter is added herein by these claim amendments. Specifically, support for the claim amendments is found in at least paragraphs 21 and 31 of the as-filed Specification.

II. Examiner Interview Summary

On January 12, 2023, Cory Smith and George Chen (attorneys for Applicant) and Alexander Dizengof (inventor of the subject application, and Founder & Chief Technology Officer of Applicant), conducted a telephonic interview with Primary Examiner Gary Lafontant regarding this Application. During this interview, the invention and amendments to overcome the rejections under 35 U.S.C. § 103 were discussed. Applicant thanks Primary Examiner Lafontant for his time and assistance on this matter.

III. Amended Claims 1-20 Are Allowable in View of 35 U.S.C. § 103

A. Amended Claims 1-20 Are Allowable over Piett and Somes

The Patent Office rejects claims 1-20 under 35 U.S.C. § 103 as being allegedly unpatentable over U.S. Patent Application Publication No. 2016/0337831 to Piett et al. (“Piett”) in view of U.S. Patent Application Publication No. 2015/0106528 to Somes et al. (“Somes”). Applicant respectfully submits that Piett and Somes, whether taken alone or in combination, do not teach or suggest every limitation of amended claims 1-20.

1. Amended Independent Claims 1, 8, and 15 Are Allowable

Amended independent claims 1, 8, and 15 require, in part, “transmitting a uniform resource locator (URL) link to the mobile device through an electronic message, wherein the electronic message is transmitted through a second connection using the phone number, . . . and sending the real-time video stream to the recipient for display on a screen of the recipient, wherein the real-time video stream is associated with a unique identifier for the mobile device.”

Piett does not teach or suggest these limitations. The Patent Office cites to Piett for teaching the pre-amended limitations, but those citations are inapposite, for the reasons explained as follows:

For the pre-amended limitation “transmitting a uniform resource locator (URL) to the mobile device through an electronic message,” the Patent Office cites to FIG. 1 (102) and paragraphs 22 and 62-65 of Piett, and asserts “mobile device received URI message to initiate transmission of data through network 106, URI comprises URL.” Office Action at 3. However, paragraph 62 of Piett teaches that the URI is “a SIP From-URI,” which is the “Uniform Resource Identifier” data in the Session Initiation Protocol (SIP). This URI is not a “uniform resource locator (URL) link,” as required by amended independent claims 1, 8, and 15. Moreover, nowhere does Piett teach or suggest “transmitting a uniform resource locator (URL) link *to the mobile device* through an electronic message” (emphasis added).

For the limitation “the electronic message is transmitted through a second connection using the phone number,” the Patent Office cites to FIG. 1 (106) and paragraphs 22, 39, 42-43, and 60-62 of Piett, and asserts “OTSL communicate with calling device via network 106.” Office Action at 3. However, paragraphs 43, 60-62 of Piett teach public safety access point (PSAP) 108 querying OTSL computing device 110 using a unique device ID, and Piett does not teach or suggest using a phone number in the communications between OTSL computing device 110 and calling device 102 through network 106, despite the Patent Office having asserted that network 106 reads on the “second connection.”

Nowhere does Piett teach or suggest “transmitting a uniform resource locator (URL) link to the mobile device through an electronic message, wherein the electronic message is transmitted through a second connection using the phone number, . . . and sending the real-time video stream to the recipient for display on a screen of the recipient, wherein the real-time video stream is associated with a unique identifier for the mobile device,” as required by amended independent claims 1, 8, and 15.

Meanwhile, *Somes* does not provide the missing teachings of Piett, whether taken alone or in combination. The Patent Office cites to *Somes* for teaching the pre-amended limitations, but those citations are inapposite, for the reasons explained as follows:

For the limitation “sending the real-time video stream to the recipient for display on a screen of the recipient,” the Patent Office cites to paragraphs 20 and 84 of *Somes*, and asserts “end user display of video.” Office Action at 5. However, paragraphs 20 and 84 of *Somes* teach sending “service data.” This “service data” is not a “real-time video stream,” as *Somes* describes “service data” as follows:

Service data may include one or multiple types of data. For example, one type of service data may pertain to the user, another type of service data may pertain to the user device of the user, yet another type of service data may pertain to another network device and/or a network, and still another type of service data may pertain to a WebRTC session setting. While these types of service data are exemplary and are not intended to be exhaustive, the acquisition and use of various types of service data may depend on various factors, such as, for example, the type of WebRTC session (e.g., video and audio, a telephone call, etc.), whether the user has an account with a service provider (e.g., a web service provider, a WebRTC service provider, etc.), whether the user is prompted to provide service data, and the other party involved in the WebRTC session. The service data may include data previously stored prior to an initiation of a WebRTC session, data obtained during the establishment of a WebRTC session, and/or data obtained during the WebRTC session. More specific examples are described below.

Somes at ¶ 13. Nowhere does Somes describe “service data” as a “real-time video stream.”

For the limitation “the real-time video stream is associated with a unique identifier for the mobile device,” the Patent Office cites to paragraphs 16-17 and 47 of Somes, and asserts “WebRTC associated with identifier of UE.” Office Action at 5. However, paragraphs 16-17 and 47 of Somes refer to “service data,” which is not the “real-time video stream,” as explained above.

Nowhere does Somes teach or suggest “transmitting a uniform resource locator (URL) link to the mobile device through an electronic message, wherein the electronic message is transmitted through a second connection using the phone number, . . . and sending the real-time video stream to the recipient for display on a screen of the recipient, wherein the real-time video stream is associated with a unique identifier for the mobile device,” as required by amended independent claims 1, 8, and 15. Accordingly, Somes does nothing to rectify the deficiencies of Piett, whether taken alone or in combination.

Accordingly, Applicant respectfully requests the allowance of amended independent claims 1, 8, and 15.

2. Dependent Claims 2-7, 9-14, and 16-20 Are Allowable

Applicant overcomes the rejection of claims 2-7, 9-14, and 16-20 under 35 U.S.C. § 103 as being allegedly unpatentable over Piett and Somes because claims 2-7, 9-14, and 16-20 depend, directly or indirectly, from amended independent claims 1, 8, or 15. Dependent claims must be construed to include all of the limitations of the claims from which they depend, as required by 37

C.F.R. § 1.75(c) and MPEP § 608.01(n). The deficiencies of Piett and Somes in relation to amended independent claims 1, 8, and 15 are discussed above. Accordingly, the Patent Office should allow dependent claims 2-7, 9-14, and 16-20 for at least the same reasons as listed earlier for amended independent claims 1, 8, and 15, as well as for their own respective limitations.

For example, claims 3, 10, and 17 are not taught by Piett or Somes, whether taken alone or in combination. The Patent Office cites to paragraph 38 of Piett, but that paragraph teaches: “It should be appreciated that other types of emergency communications (e.g., text messages) can be transmitted via the *cellular communications network 104* as described herein” (emphasis added). Importantly, claim 1 recites “the electronic message is transmitted through a second connection using the phone number,” and the Patent Office has asserted the second connection is network 106, not cellular communications network 104. Nowhere do Piett or Somes teach or suggest “the electronic message is a text message,” as required by claims 3, 10, and 17.

As another example, claims 6, 13, and 19 are not taught by Piett or Somes, whether taken alone or in combination. The Patent Office cites to paragraphs 42-44 and 48-49 of Somes, but those paragraphs teach converting the format of the service data, which is not the “real-time video stream,” as explained above. Nowhere do Piett or Somes teach or suggest “the server is a proxy server configured to convert a data format of the real-time video stream,” as required by claims 6, 13, and 19.

As a further example, claims 7, 14, and 20 are not taught by Piett or Somes, whether taken alone or in combination. The Patent Office cites to paragraphs 25, 43, and 60 of Piett, which teach an app pushing location data, not a WebRTC session transmitting GPS location data. Nowhere do Piett or Somes teach or suggest “the WebRTC session further transmits at least one of (i) GPS location data of the mobile device for display on the screen of the recipient or (ii) one or more photographs taken on the mobile device for display on the screen of the recipient,” as required by claims 7, 14, and 20.

IV. The References Cited in the European Opposition Do Not Appear to Fully Teach or Suggest the Limitations of Amended Claims 1-20

Applicant calls the Patent Office’s attention to the Information Disclosure Statement (IDS) submissions filed by Applicant on January 6, 2023 and February 23, 2023, in which some of the references relate to the 999EYE system. All of the references cited in these two IDS submissions, except for WO 2014158562, were cited or included in an Opposition filed December 9, 2022 in

European Patent No. EP 3 445 016, which is owned by Applicant and claims priority to U.S. Provisional Application No. 62/544,835, to which this instant application also claims priority. The Opposition argues, regarding the 999EYE system, that: “[a]s the user devices are capable of initiating a stream without a dedicated app via a ‘*web portal*’ by clicking on a URL, it is clear that the system makes use of the smartphone’s in-built web browser,” and “[c]learly the ‘*web portal*’ described . . . indicates the presence of a WebRTC to facilitate the streaming session.” Opposition at § 4.24 (emphasis in original). A third party has notified Applicant of similar allegations. However, such references regarding the 999EYE system do not appear to clearly disclose that the 999EYE system uses the WebRTC technology. Accordingly, Applicant asserts that the references regarding the 999EYE system do not appear to fully teach or suggest the limitations of amended claims 1-20.

CONCLUSION

Applicant has made an earnest attempt to place this case in condition for allowance. In light of the amended claims and remarks set forth above, Applicant respectfully requests consideration and allowance of all of the pending claims.

As Applicant's remarks with respect to the Patent Office's rejections are sufficient to overcome these rejections, Applicant's silence as to certain assertions or requirements applicable to such rejections (e.g., whether a reference constitutes prior art, whether a reference shows, discloses, teaches, or suggests a claim limitation, whether a reference is non-analogous art, motivation to combine references, etc.) is not a concession by Applicant that such assertions are accurate or such requirements have been met, and Applicant reserves the right to analyze and dispute the same in the future. Also, Applicant asserts that no one should construe any contents of this paper as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment or cancellation of any claim does not necessarily signify a concession of unpatentability of the claim prior to its amendment.

Applicant believes no fees are due in connection with this Response to Office Action. However, the Commissioner for Patents is hereby authorized to charge any additional fees necessitated by the filing of this paper, or credit any overpayment, to Account No. 02-4467.

If matters can be discussed by telephone to further the prosecution of this application, Applicant invites the Examiner to call the undersigned attorney at the Examiner's convenience.

Respectfully submitted,

BRYAN CAVE LEIGHTON PAISNER LLP
Two North Central Avenue
Suite 2100
Phoenix, AZ 85004-4406

By: /Cory G. Smith/
Cory G. Smith
Attorney for Applicant
Reg. No. 63,218
Tel. (602) 364-7442

Electronic Acknowledgement Receipt

EFS ID:	47585375
Application Number:	17943956
International Application Number:	
Confirmation Number:	2316
Title of Invention:	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE
First Named Inventor/Applicant Name:	Alexander Dizengof
Customer Number:	46019
Filer:	Cory Smith/Lisa Mansur
Filer Authorized By:	Cory Smith
Attorney Docket Number:	3010043.2
Receipt Date:	24-FEB-2023
Filing Date:	13-SEP-2022
Time Stamp:	15:09:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		3010043-000002-Response-to-Office-Action.pdf	207850 a834f29651c937845469084aca71083ecd26867d	yes	13

Multipart Description/PDF files in .zip description		
Document Description	Start	End
Amendment/Request for Reconsideration-After Non-Final Rejection	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	13

Warnings:

Information:

Total Files Size (in bytes):	207850
-------------------------------------	--------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 17/943,956	Filing Date 09/13/2022	<input type="checkbox"/> To be Mailed
---	--	---------------------------	---------------------------------------

ENTITY: LARGE SMALL MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 = *		x \$50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 = *		x \$240 =	
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL

APPLICATION AS AMENDED - PART II

	(Column 1)		(Column 2)	(Column 3)	RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT	02/24/2023		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	x \$40 = 0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	x \$192 = 0
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))					
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE
						0

	(Column 1)		(Column 2)	(Column 3)	RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT			CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$0 =
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$0 =
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))					
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE
						LIE

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, 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.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

U.S. PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S. PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1	20150056946	A1	2015-02-26	Leggett et al.			
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2014182638	WO	A2	2014-11-13	Decharms		
If you wish to add additional Foreign Patent Document citation information please click the Add button.							Add	
NON-PATENT LITERATURE DOCUMENTS							Remove	
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.						T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

1	"Notice of Opposition of a European Patent," filed in EP Patent No. 3,445,016, by Dentons UK and Middle East LLP, dated December 9, 2022.
---	---

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- See attached certification statement.
- The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Cory Smith/	Date (YYYY-MM-DD)	2023-02-23
Name/Print	Cory Smith	Registration Number	63218

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour 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. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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.

Electronic Patent Application Fee Transmittal

Application Number:	17943956				
Filing Date:	13-Sep-2022				
Title of Invention:	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE				
First Named Inventor/Applicant Name:	Alexander Dizengof				
Filer:	Cory Smith/Lisa Mansur				
Attorney Docket Number:	3010043.2				
Filed as Small Entity					
Filing Fees for Utility under 35 USC 111(a)					
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)	
Basic Filing:					
Pages:					
Claims:					
Miscellaneous-Filing:					
Petition:					
Patent-Appeals-and-Interference:					
Post-Allowance-and-Post-Issuance:					
Extension-of-Time:					

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	104	104
Total in USD (\$)				104

Electronic Acknowledgement Receipt

EFS ID:	47578168
Application Number:	17943956
International Application Number:	
Confirmation Number:	2316
Title of Invention:	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE
First Named Inventor/Applicant Name:	Alexander Dizengof
Customer Number:	46019
Filer:	Cory Smith/Lisa Mansur
Filer Authorized By:	Cory Smith
Attorney Docket Number:	3010043.2
Receipt Date:	23-FEB-2023
Filing Date:	13-SEP-2022
Time Stamp:	12:02:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$104
RAM confirmation Number	E20232MC03029484
Deposit Account	024467
Authorized User	Lisa Mansur

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)
 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	WO-2014182638A2.pdf	5923093	no	144
			2d37fb14c404b7d94b1fdb5d042e59fee2c b8b7c		
Warnings:					
Information:					
2	Non Patent Literature	NPL-1.pdf	1268675	no	19
			fc13ad70940378fc3700a5e8f466dd658c8b e75d		
Warnings:					
Information:					
3	Transmittal Letter	3010043-000002-IDS- Transmittal-Letter.pdf	97343	no	1
			cf0bd5ed88e314175bc6586d41470444ce5 20492		
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Form (SB08)	3010043-000002-IDS-Form.pdf	1034219	no	4
			bb6203d0b4693ac0850e7b062b36fd9636 d521a		
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	38344	no	2
			3308d97e6c786bd3194e23f40c83bb9bbb 6721f9		
Warnings:					
Information:					
Total Files Size (in bytes):			8361674		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



Espacenet

Bibliographic data: WO2014182638 (A2) — 2014-11-13

MOBILE SECURITY TECHNOLOGY

Inventor(s): DECHARMS CHRISTOPHER [US] ± (DECHARMS, CHRISTOPHER)

Applicant(s): DECHARMS CHRISTOPHER [US] ± (DECHARMS, CHRISTOPHER)

Classification: - international: H04W4/90
 - cooperative: G06Q50/265 (EP, US); H04L65/1059 (EP, US); H04L65/1069 (EP, US); H04L65/1096 (EP, US); H04L65/403 (EP, US); H04L67/52 (EP, US); H04L67/55 (US); H04M1/72418 (EP, US); H04N7/147 (EP, US); H04N7/148 (US); H04N7/15 (US); H04W4/02 (EP); H04W4/021 (EP, US); H04W4/029 (US); H04W4/90 (EP, US); H04W76/14 (EP, US); H04M2201/50 (EP, US); H04M2203/306 (EP, US); H04M2242/04 (EP, US); H04M2242/30 (EP, US); H04M3/567 (EP, US)

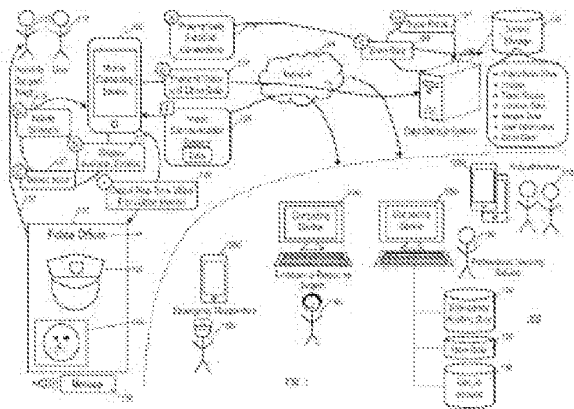
Application number: WO2014US36871 20140505 [Global Dossier](#)

Priority number(s): [US201361819575P 20130504](#) ; [US201361872690P 20130831](#) ; [US201461924901P 20140108](#)

Also published as: [WO2014182638 \(A3\)](#) [AU2014262897 \(A1\)](#) [AU2014262897 \(B2\)](#) [CA2947936 \(A1\)](#) [EP2992692 \(A2\)](#) [more](#)

Abstract of WO2014182638 (A2)

In one implementation, a computer-implemented method includes determining a location of a mobile computing device using one or more of a plurality of data sources; communicating, by the mobile computing device, with another computing device as part of a two-way video chat session over a first network connection, the communicating including transmitting the location of the mobile computing device; displaying, as part of the two-way video chat session, real-time video from the other computing device; recording video using one or more cameras that are accessible to the mobile computing device; and transmitting, over a second network connection, the video to a remote storage system for persistent storage.





- (51) International Patent Classification: Not classified
- (21) International Application Number: PCT/US2014/036871
- (22) International Filing Date: 5 May 2014 (05.05.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:

61/819,575	4 May 2013 (04.05.2013)	US
61/872,690	31 August 2013 (31.08.2013)	US
61/924,901	8 January 2014 (08.01.2014)	US
- (72) Inventor; and
- (71) Applicant : **DECHARMS, Christopher** [US/US]; Box 370786, Montara, California 94037 (US).
- (74) Agent: **HOFF, Christopher**; Krenz Hoff, LLP, 10800 Lyndale Avenue South, Suite 163, 10800 Lyndale Avenue South, Bloomington, Minnesota 54420 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,

BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report (Rule 48.2(g))

(54) Title: MOBILE SECURITY TECHNOLOGY

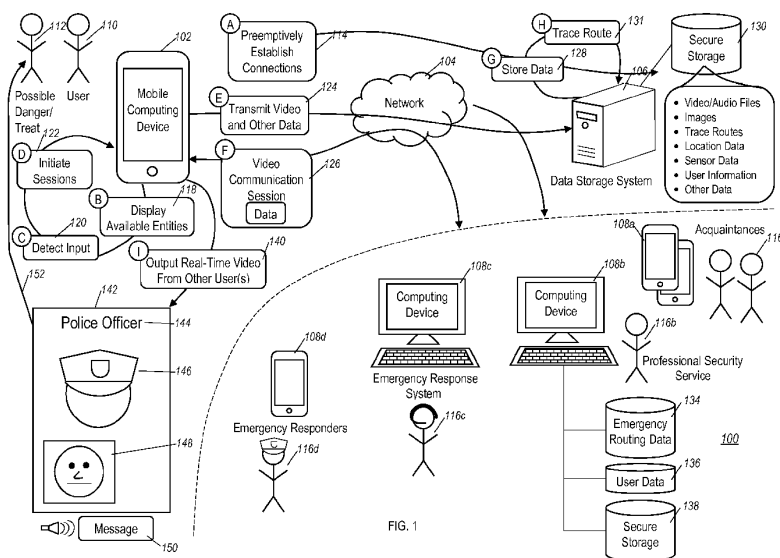


FIG. 1

(57) Abstract: In one implementation, a computer-implemented method includes determining a location of a mobile computing device using one or more of a plurality of data sources; communicating, by the mobile computing device, with another computing device as part of a two-way video chat session over a first network connection, the communicating including transmitting the location of the mobile computing device; displaying, as part of the two-way video chat session, real-time video from the other computing device; recording video using one or more cameras that are accessible to the mobile computing device; and transmitting, over a second network connection, the video to a remote storage system for persistent storage.

WO 2014/182638 A2

MOBILE SECURITY TECHNOLOGY

Cross-Reference to Related Applications

This application claims priority to U.S. Provisional Application Serial No. 61/819,575, which is entitled "Mobile Security Technology" and was filed on May 4, 2013; to U.S. Provisional Application Serial No. 61/872,690, which is entitled "Mobile Security Technology" and was filed on August 31, 2013; and to U.S. Provisional Application Serial No. 61/924,901, which is entitled "Mobile Security Technology" and was filed on January 8, 2014, the entire contents of which are hereby incorporated by reference.

Technical Field

This document generally describes computer-based technologies related to security. For example, this document describes, among other things, mobile computing devices that provide security features through the use of a variety of computer-based technologies, such as one-way, two-way, or multi-party video chat and/or video conferencing technology.

Background

Computer-based technologies have been used for security and video surveillance. For example, computer-based technology has been developed allow for users to stream live video feeds from security cameras over the internet and on remote computing devices, such as laptop computers, desktop computers, and mobile computing devices.

Summary

This document generally describes computer-based technologies to provide security and assistance to users whenever they are in need of such services, such as when users are in dangerous or uncertain physical situations in which their safety or the safety of others may be in jeopardy. For example, the disclosed technologies can allow for users to quickly obtain access to and to involve appropriate remote parties in their current physical

situation in an effort to avoid any harm from befalling the users, while at the same time storing information (e.g., video recording) regarding the incident at a secure and remote storage facility. Such access and involvement of remote parties can be provided through the use of any of a variety of appropriate techniques, such as two-way remote monitoring, remote imaging, audio and video conferencing and remote control technology on mobile computing devices, such as cell phones, smartphones, personal digital assistants (PDAs), tablets, wearable computing devices (e.g., GOOGLE GLASS, Looxcie, GoPro), and/or other devices that can provide connection between users and increase users security. For example, a user may initiate two-way video conferencing with a friend, police, or emergency responder as a means of allowing the responder to help facilitate a secure outcome for the user.

Implementations of the disclosed technology can be methods that include one or more of the following features: two-way audiovisual teleconferencing between two computing devices over a network connection (A); transmitting and receiving, by an application running on a mobile computing device, real-time audio and video with another computing device over a network connection (B); communicating, by a mobile computing device, with another computing device as part of a two-way video chat session over a network connection; and displaying, as part of the two-way video chat session, real-time video from the other computing device while transmitting real-time video from the mobile computing device to the other computing device (C); the network connection can be a peer-to-peer connection (D); identifying a plurality of candidate responders, and selecting a particular candidate responder based, at least in part, on one or more factors (E); the factors can include one or more of: a user location, a responder location, responder ratings, responder skills and/or training, type of situation, and a predefined list of responders (F); determining a location of a mobile computing device using one or more of a plurality of data sources (G); the data sources can include one or more of: GPS, WiFi, beacon signals, other data transmitted by radiofrequency that is useable to electronically locate a device (H); determining or receiving a geographic location for a user, and identifying, using a database of locations and corresponding responders, one or more

appropriate responders based, at least in part, on said geographic location (I); the database of locations can be a PSAP database (J); receiving a geographic location for a user, and determining, using a database of locations and corresponding licensure status, whether said user is located within one or more licensed jurisdictions (L); the licensed jurisdiction can include an area where an entity has been granted a right to perform a service (M); receiving a request to connect a mobile computing device with a responder service, identifying an appropriate responder service based on the location of the mobile computing device, and initiating contact with the appropriate responder service on behalf of the mobile computing device (N); the request can be one or more of: a text message, a verbal request, selection of call 911 feature, and can be received over peer-to-peer network connection (O); the location can be one or more of a geolocation and real-time location updates (P); initiating contact can include one or more of: establish communication session between mobile device and emergency service, and communication on behalf of the mobile computing device (Q); the responder service can be an emergency dispatch system (R); receiving a message and the location of the mobile computing device of a user, determining an appropriate emergency responder service based on the location, initiating a telephone call to appropriate the emergency responder service on behalf of the user, and transmitting the message to the emergency responder service (S); the message can be sent with one or more of the user's profile and the user's contact information, and can be included with initiating three-way communication with the user (T); receiving a text message requesting emergency responder services for a user of a mobile computing device, the text message identifying a location of the mobile computing device, determining an appropriate emergency responder service based on the location, and initiating a telephone call to appropriate the emergency responder service on behalf of the user (U); receiving a message and the location of the mobile computing device of a user, determining an appropriate responder service based on the location, initiating electronic communication with the appropriate the responder service for the user, and transmitting the message to the responder service (V); the electronic communication can include one or more of: communication between the mobile

computing device and the emergency responder service, communication between the central system and the emergency responder service, and the electronic communication can include information about the user (W); the responder service can be an emergency dispatch system (X); providing the user's profile, providing the user's contact information, and/or initiating three-way communication with the user (Y); recording video using one or more cameras that are accessible to a computing device, modifying the video by adding one or more features, and transmitting the modified video with the features to a remote storage system for persistent storage (Z); the one or more cameras can include cameras connected to the computing device and wirelessly connected to the computing device (AA); the features can include one or more of: identifying features, security features, and verification features (AB); the identifying features can include user identification (AC); the security features can include encryption (AD); the verification features can include one or more of: a timestamp, a digital watermark, and location information (AE); recording a video using one or more cameras mounted to a user's body that are accessible to a computing device (AF); receiving data recorded by a computing device during an incident, identifying one or more features from the data, and determining an identity of an assailant involved in the incident based on comparison of the one or more features with information stored in one or more data sources (AG); the data can include one or more of: video data, image data, audio data, and other data detected from wireless devices (AH); the features can include one or more of: face, voice, gait, proportions, and device identity (AI); the data sources can include one or more of: criminal databases, law enforcement data sources, social network data sources, and user data (AJ); the user data can include one or more of contacts, friend lists, and a user's images (AK); recording video using one or more security cameras that are accessible to a mobile computing device, and transmitting the video to a remote storage system for persistent storage (AL); the security cameras can include one or more of remote camera and camera acting in security camera mode (AM); receiving, at a computing device, input to send a push notification to another device, determining a current location of the computing device, and transmitting a push notification to the other device that includes the current location (AN); the other device

can be specified by user input or determined based on multifactor input (AO); receiving, at a computing device, input to send a push notification to another device, determining a current location of the other device, determining whether the other device's current location is within a specified distance from a specified location, and if the other device's current location is within a specified distance from a specified location, transmitting a push notification to the other device that includes the current location (AP); receiving, at a computing device, a location of a responder through a network connection, and displaying the location of the responder on the computing device (AQ); the network connection can be received while concurrent video chat going on (AR); displaying the location can include one or more of: the location being displayed on map, icon depicting responder displayed on map, image of responder displayed on map, map presented with video feed, and location presented with regard to location of user device (AS); receiving information determining whether responders are currently available for a user of a computing device, and if no responders are currently available, taking an appropriate action (AT); the appropriate action can include one or more of: presenting a message on the computing device that no responders are available, providing information to user relating to alternate actions, and routing user's request(s) to a backup solution (AU); presenting can include one or more of: visual display, audio output, and haptic feedback (AV); receiving information determining whether responders are currently available for a user of a computing device, and if no responders are currently available, presenting a warning message on the computing device that no responders are available (AW); establishing, before initiating a communication session at a computing device, peer-to-peer network connections with a plurality of other devices associated with candidate responders, and obtaining and displaying, using the network connections, current status information for a plurality of candidate responders (AX); establishing, before initiating a two-way audiovisual communication session at a computing device, peer-to-peer network connections with a plurality of other devices associated with candidate responders, and obtaining and displaying, using the network connections, one-way video depicting a plurality of candidate responders (AY); receiving, at a computing device and

from a responder computing device, instructions to perform one or more operations, determining whether the responder computing device is permitted to remotely control operation of the computing device, and performing, based on the determining, the one or more operation (AZ); operations can include one or more of: initiating a communication session with another computing device, initiating an audio communication session with another computing device, initiating a two-way audiovisual communication session with another computing device, initiating a one-way audiovisual communication session with another computing device, activating/deactivating one or more devices (camera, microphone, audio volume, light), recording video, taking a picture, playing an alarm, playing a pre-recorded message, and outputting image/audio/video (BA); displaying a map that depicts geographically associated crime information (BB); displaying a map that depicts geographically associated crime information, receiving new crime information in substantially real time, and updating the map to additionally depict the new crime information (BC); outputting, when the location associated with the new crime information is within a threshold distance from the user's current location, information to the user (BD); transmitting a request to a computer system for a network address of another computing device, receiving, from the computer system, the network address, and establishing, using the network address, a peer-to-peer network connection with the other computing device (BE); receiving input to connect to each member of a group of users, obtaining network addresses for devices associated with the members of the group of users, and sending messages requesting network connections with the devices using the network addresses (BF); the group of users can include one or more of: friends, responders, emergency personnel, and user from designated lists (BG); providing, on a mobile computing device, an interface through which the mobile computing device acts as a user device in personal emergency response system, determining that an input received through the interface is one of a plurality of designated inputs to initiate communication with an emergency response system, and initiating, based on the determining, communication with the emergency response system (BH); recording, by a mobile computing device mounted within a user's home,

video by using a camera of the mobile computing device, and transmitting the video to a computer system with additional data obtained by the mobile computing device (BI); the additional data can include location information and user information (BJ); obtaining status information for a one or more users that are associated with one or more computing devices, and outputting the status information (BK); the status information can include an image of the user, a video of the user, whether the user is available, whether the user is on a call, whether the user is away, and whether the user is actively using the device (BL); receiving location information for a user associated with a computing device, determining, using the location information, whether the user has crossed over a boundary of a defined geographic area, and outputting an alert in response to the determining (BM); providing, by a computer system, communication operating across a plurality of different computing platforms and operating systems (BN); the computing platforms and operating systems can include one or more of: iOS, Android, Windows, WindowsMobile, Blackberry, and MacOS (BO); receiving, at a computing device associated with a user and from a responder device, instructions to contact a friend of the user, identifying an appropriate friend to contact, and initiating a communication session with a computing device associated with the identified friend (BP); encrypting, by a computing device, real-time data with associated metadata that identifies when, where, or by whom the real-time data was collected, and transmitting the real-time data (BQ); a central computer system can be a professional emergency response system (BR); gating access to one or more security features based on subscription levels for users (BS); obtaining network addresses for computing devices associated with a user's friends, and automatically initiating network connections with the computing devices (BT); sending and receiving, by a computing device, text messages with other computing devices, and displaying the text messages on the computing device (BU); detecting wireless signals from other nearby devices, and recording and transmitting information regarding the detected wireless signals and the other devices (BV); displaying on a map the locations of users #2 who have begun using an application based on a recommendation from the user in color #1, and displaying on a map the locations of users who have begun using a mobile

application based on a recommendation from the users #2 in color #2 (BW); displaying on a map the locations of users who have begun using a mobile application based on a recommendation from the users #3 in color #3 (BX); displaying on a map the locations of users who have begun using a mobile application based on a recommendation from the users #4 in color #4 (BY); the application can include one or more of: a security application, a social networking application, and an application that was either directly or indirectly provided to the users (BZ); receiving a current location for a user, determining a current safety level for the user at the current location based on one or more factors (CA); the factors can include one or more of: location, crime information, current time, user's profile, user's age, user's gender, available responders, and proximity of responders to the user (CB); a communication protocol that is used can be webRTC (CC); selecting, from among a plurality of responders, one or more responders based, at least in part, on user-generated ratings for the plurality of responders (CD); outputting a graphical user interface element can include a slider through which a user can browse a group of users through linear swiping inputs (CE); receiving a request to transmit a location to another computing device, determining the location of the computing device, and transmitting the location to another computing device (CF); a data source from which user contact information and location information is obtained can be social media (CG); information can be transmitted through a social media platform (CH); receiving input describing an incident, collecting additional details detected or sensed by the mobile computing device regarding the incident, and reporting the incident using the input and the additional details (CI); the additional details can include one or more of: geographic location, images, and video (CJ); information regarding a user can be stored as a user profile (CK); and displaying a video instructing a user how to operate a mobile security application (CL).

The features A-CL can be combined in any of a variety of appropriate ways. For example, the features A-CL, including all possible subsets thereof, can be used in every possible combination and in every possible permutation.

Implementations of the disclosed technology can be computing devices and/or computer systems that include one or more of the following features: means to engage in two-way audiovisual teleconferencing with another computing device through a network (CM); means to capture an audio and video datastream #1 (CN); means to transfer said audio and video datastream #1 to another computing device (CO); means to receive audio and video datastream #2 from another computing device (CP); means to display video from said audio and video datastream #2 (CQ); means to present audio from said audio and video datastream #2 (CR); means to receive audio and video from another computing device (CS); a camera, a network interface that is programmed to transmit real-time video recorded by camera to another computing device over a network connection, and to receive real-time video recorded by the other computing device, and a display that is programmed to display, concurrently with transmitting the real-time video, the real-time from the other computing device (CT); a camera, a network interface that is programmed to communicate with another computing device as part of a two-way video chat session over a network connection, and a display that is programmed to display, as part of the two-way video chat session, real-time video from the other computing device while transmitting real-time video from the mobile computing device to the other computing device (CU); a mobile security application that is programmed to identify a plurality of candidate responders; and select a particular candidate responder based, at least in part, on one or more factors (CV); a geographic location unit that is programmed to determine a location of a mobile computing device using one or more of a plurality of data sources (CW); a network interface that is programmed to receive a geographic location for a user, a database of locations and corresponding responders, and a routing system programmed to identify one or more appropriate responders based, at least in part, on the geographic location for said user and said database (CX); a jurisdiction module that is programmed to determine, for an assistance request for a user, whether the user is located within one or more licensing jurisdictions, and a responder identification module that is programmed to identify a responder to provide assistance to the user based on the determination of whether the user is located within the licensing

jurisdictions (CY); a network interface that is programmed to receive a request to connect a mobile computing device with an responder service, an emergency routing system that is programmed to identify an appropriate emergency responder service based on the location of the mobile computing device, and connection manager that is programmed to initiate contact with the appropriate emergency responder service on behalf of the mobile computing device (CZ); a network interface that is programmed to receive a message from a mobile computing device, the message including a location of the mobile computing device, a routing system that is programmed to determine an appropriate responder service based on the location, and connection manager that is programmed to initiate a telephone call to appropriate the emergency responder service on behalf of the user (DA); a network interface that is programmed to receive a message from a mobile computing device, the message including a location of the mobile computing device, a routing system that is programmed to determine an appropriate responder service based on the location, and connection manager that is programmed to initiate electronic communication with the appropriate the responder service for the user and transmit the message (DB); one or more cameras that are programmed to record video, a security layer that is configured to modify the video to add one or more features, and a network interface that is configured to transmit the modified video with the features to a remote storage system for persistent storage (DC); one or more cameras mounted to a user's body that are accessible to a computing device (DD); a network interface that is programmed to receive data recorded by a computing device during an incident, a feature identification module that is programmed to identify one or more features from the data, and an assailant identifier that is programmed to determine an identity of an assailant involved in the incident based on comparison of the one or more features with information stored in one or more data sources (DE); one or more security cameras that are configured to record video on a mobile computing device, and a network interface that is programmed to transmit the video to a remote storage system for persistent storage (DF); a user interface that is programmed to receive input to send a push notification to another device, a location unit that is programmed to determine a current

location of the computing device, and a network interface that is programmed to transmit a push notification to the other device that includes the current location (DG); a user interface that is programmed to receive input to send a push notification to another device, a location unit that is programmed to determine a current location of the computing device, and a network interface that is programmed to transmit a push notification to the other device that includes the current location (DH); a network interface that is programmed to receive a location of a responder through a network connection, and a display that is configured to display the location of the responder on the computing device (DI); a network interface that is configured to receive information indicating that no responders are currently available for a user of a computing device, and an output subsystem that is configured to output a warning message on the computing device that no responders are available (DJ); a network interface that is configured to establish, before initiating a communication session and at a computing device, peer-to-peer network connections with a plurality of other devices associated with candidate responders, a status module that is programmed to obtain using the network connections, current status information for a plurality of candidate responders, and a display that is configured to display the current status information for a plurality of candidate responders (DK); a network interface that is configured to establish, before initiating two-way audiovisual communication session and at a computing device, peer-to-peer network connections with a plurality of other devices associated with candidate responders, a status module that is programmed to obtain using the network connections, current status information for the candidate responders, and a display that is configured to display the current status information for the candidate responders (DL); a network interface that is configured to receive, from a responder computing device, instructions to perform one or more operations, a permissions module that is configured to determine whether the responder computing device is permitted to remotely control operation of the computing device, and a processor that is configured to perform, based on the determining, the one or more operation (DM); a display that is programmed to display a map that depicts geographically associated crime information (DN); a display

that is programmed to display a map that depicts geographically associated crime information, a network interface that is programmed to receive, in real-time and while displaying the map, new crime information, wherein the map is updated to additionally depict the new crime information, and an output subsystem that is programmed to output, when the new crime information is within a threshold distance, a notification (DO); a network interface that is programmed to: transmit a request to a computer system for a network address of another computing device, receive the network address, and establish, using the network address, a peer-to-peer network connection with the other computing device (DP); a user interface that is configured to receive input to connect to each member of a group of users, and a network interface that is programmed to obtain network addresses for devices associated with the members of the group of users, and sending messages requesting initiating network connections with the devices using the network addresses (DQ); an interface through which the mobile computing device acts as a user device in personal emergency response system, an input interpreter that is programmed to determine that an input received through the interface is one of a plurality of designated inputs to initiate communication with an emergency response system, and a network interface that is programmed to initiate, based on the determining, communication with the emergency response system (DR); an in-home mount, a mobile computing device that is sized to fit within the in-home mount, the mobile computing device including: a camera, a video recording module that is programmed to record video using the, and a network interface that is programmed to transmit the video to a computer system with additional data obtained by the mobile computing device (DS); a network interface that is programmed to obtain status information for a one or more users that are associated with one or more computing devices, and an output subsystem that is programmed to output the status information (DT); a network interface that is programmed to receive location information for a user associated with a computing device, a location tracking module that is programmed to determine, using the location information, whether the user has crossed over a boundary of a defined geographic area, and an alert module that is programmed to output an alert

in response to the determining (DU); a network interface that is configured to provide security features to computing devices operating across a plurality of different computing platforms and operating systems (DV); a network interface that is programmed to receive, from a responder device, instructions to contact a friend of a user, a contact identification module that is programmed to identify an appropriate friend to contact, and wherein the network interface is further programmed to initiate a communication session with a computing device associated with the identified friend (DW); a security module that is programmed to encrypt real-time data with associated metadata that identifies when, where, or by whom the real-time data was collected, and a network interface that is programmed to transmit the real-time data (DX); a central computer system comprises a professional emergency response system (DY); a subscription module that is programmed to gate access to one or more security features based on subscription levels for users (DZ); a text messaging module that is programmed to send and receive text messages with other computing devices, and a user interface that is programmed to display the text messages on the computing device (EA); a wireless transceiver that is configured to detect nearby wireless signals from other devices, and a network interface that is programmed to transmit information regarding the detected wireless signals and the other devices (EB); a display that is programmed to display a map that depicts color coded regions that correspond to users who have begun using a mobile security application based on a recommendation from the user that was either directly or indirectly provided to the users (EC); a network interface that is programmed to receive a current location for a user, and a safety module that is programmed to determine a current safety level for the user at the current location based on one or more factors (ED); wherein a communication protocol that is used comprises webRTC (EE); a responder selection module that is programmed to select, from among a plurality of responders, one or more responders based, at least in part, on user-generated ratings for the plurality of responders (EF); a user interface that includes a graphical element comprising a slider through which a user can browse a group of users through linear swiping inputs (EG); a user interface that is programmed to receive a request to transmit a location to another

computing device, a location unit that is programmed to determine the location of the computing device, and a network interface that is programmed to transmit the location to another computing device (EH); a data source from which user contact information and location information is obtained comprises social media (EI); a user interface that is programmed to receive input describing an incident, an input subsystem that is configured to collect additional details detected or sensed by the mobile computing device regarding the incident, and a network interface that is programmed to report the incident using the input and the additional details (EJ); information regarding a user is stored as a user profile (EK); and a display that is configured to display a video instructing a user how to operate a mobile security application (EL).

The features CM-EL can be combined in any of a variety of appropriate ways, including with the features A-CL. For example, the features A-EL, including all possible subsets thereof, can be used in every possible combination and in every possible permutation.

In one implementation, a computer-implemented method includes determining a location of a mobile computing device using one or more of a plurality of data sources; identifying a plurality of candidate responders; selecting a particular candidate responder based, at least in part, on one or more factors; and initiating two-way audiovisual teleconferencing between the mobile computing device and the particular candidate responder over a network connection. The method can include one or more of the following features, which can be used in any possible combinations. The network connection can be a peer-to-peer connection. The factors can include one or more of the following: user location, responder location, responder ratings, responder skills/training, type of situation, and a predefined list of responders. The data sources include one or more of the following: GPS, WiFi, beacon signals, other data transmitted by radiofrequency that is useable to electronically locate a device. Receiving a geographic location for a user, and determining, using a database of locations and corresponding licensure status, whether said user is located within one or more licensed jurisdiction. Determining or receiving a geographic location for a user, and identifying, using a

database of locations and corresponding responders, one or more appropriate responders based, at least in part, on said geographic location. Receiving a request to connect a mobile computing device with a responder service, identifying an appropriate responder service based on the location of the mobile computing device, and initiating contact with the appropriate responder service on behalf of the mobile computing device. Receiving, at a computing device, a location of a responder through a network connection; and displaying the location of the responder on the computing device. Receiving information determining whether responders are currently available for a user of a computing device; and if no responders are currently available, taking an appropriate action. Establishing, before initiating a communication session at a computing device, peer-to-peer network connections with a plurality of other devices associated with candidate responders; and obtaining and displaying, using the network connections, current status information for a plurality of candidate responders. Recording video using one or more cameras that are accessible to a computing device; modifying the video by adding one or more features; and transmitting the modified video with the features to a remote storage system for persistent storage. Receiving a current location for a user; and determining a current safety level for the user at the current location based on one or more factors.

In another implementation, a computing device includes a geographic location unit that is programmed to determine a location of a mobile computing device using one or more of a plurality of data sources; a mobile security application that is programmed to identify a plurality of candidate responders and to select a particular candidate responder based, at least in part, on one or more factors; a camera; a network interface that is programmed to transmit real-time video recorded by camera to another computing device associated with the particular candidate responder over a network connection, and to receive real-time video recorded by the other computing device; and a display that is programmed to display, concurrently with transmitting the real-time video, the real-time from the other computing device.

In another implementation, a computer-implemented method includes communicating, by a mobile computing device, with another computing device as part of a two-way video chat session over a network connection; displaying, as part of the two-way video chat session, real-time video from the other computing device while transmitting real-time video from the mobile computing device to the other computing device; receiving a request to connect a mobile computing device with a responder service; identifying an appropriate responder service based on the location of the mobile computing device; initiating contact with the appropriate responder service on behalf of the mobile computing device; recording video using one or more cameras that are accessible to a computing device; modifying the video by adding one or more features; and transmitting the modified video with the features to a remote storage system for persistent storage. The method can include one or more of the following features, which can be used in any possible combinations. Receiving, at a computing device, a location of a responder through a network connection; and displaying the location of the responder on the computing device. Receiving information determining whether responders are currently available for a user of a computing device; and if no responders are currently available, taking an appropriate action. Establishing, before initiating a communication session at a computing device, peer-to-peer network connections with a plurality of other devices associated with candidate responders; and obtaining and displaying, using the network connections, current status information for a plurality of candidate responders. Receiving a current location for a user; determining a current safety level for the user at the current location based on one or more factors. A communication protocol that is used comprises webRTC. Encrypting, by a computing device, real-time data with associated metadata that identifies when, where, or by whom the real-time data was collected; and transmitting the real-time data.

In another implementation, a computer-implemented method includes determining a location of a mobile computing device using one or more of a plurality of data sources; communicating, by the mobile computing device, with another computing device as part of a two-way video chat session over a first network connection, the communicating

including transmitting the location of the mobile computing device; displaying, as part of the two-way video chat session, real-time video from the other computing device; recording video using one or more cameras that are accessible to the mobile computing device; and transmitting, over a second network connection, the video to a remote storage system for persistent storage.

The method can optionally include one or more of the following features. The method can further include identifying from a data source a plurality of potential responder computing devices associated with candidate responders; and automatically selecting a particular potential responder computing device to communicate with that is associated with a particular potential candidate responder based, at least in part, on one or more factors including the availability of the responder for communication. The method can also include receiving, at the mobile computing device, a location of a responder through a network connection; and displaying the location of the responder on the mobile computing device. The method can additionally include receiving information that indicates whether responders are currently available for a user of the mobile computing device; and if it is detected that no responders are currently available, taking an appropriate alternate action. The method can further include establishing, before initiating the communication session at the other computing device, network connections with a plurality of other devices associated with candidate responders; and obtaining and displaying, using the network connections, current status information for a plurality of candidate responders. The method can also include receiving, at the mobile computing device and from a responder computing device, instructions to perform one or more operations; determining whether the responder computing device is permitted to remotely control operation of the mobile computing device; and if the responder computing device is permitted to remotely control operation of the mobile computing device based on the determining, performing, the one or more operations. The method can additionally include encrypting, by the mobile computing device, real-time data with associated metadata that identifies when, where, or by whom the real-time data was collected; and transmitting the real-time data. The method can also include receiving a

current location for a user; and determining a current safety level for the user at the current location based on one or more factors including the location. A communication protocol that is used comprises webRTC.

In another implementation, a computing device includes one or more cameras that are programmed to record video; a geographic location unit that is programmed to determine a location of a computing device using one or more of a plurality of data sources; a network interface that is programmed to communicate with another computing device as part of a two-way video chat session over a first network connection and to cause the video to be transmitted, over a second network connection, to a remote storage system for persistent storage, the location of the computing device being sent over the first and second network connections; and a display that is programmed to display, as part of the two-way video chat session, real-time video from the other computing device.

The computing device can optionally include one or more of the following features. The computing device can further include a security application that is programmed to identify a plurality of candidate responders and to select a particular candidate responder based, at least in part, on one or more factors, wherein the particular candidate responder is associated with the other computing device. The network interface can be further programmed to establish, before initiating the communication with the other computing device, network connections with a plurality of other computing devices associated with candidate responders; the device can further include a status module that is programmed to obtain, using the network connections, current status information for a plurality of candidate responders; and the display can further be programmed to display the current status information for a plurality of candidate responders. The network interface can further be programmed to receive, from a responder computing device, instructions to perform one or more operations; the computing device can further include a permissions module that is programmed to determine whether the responder computing device is permitted to remotely control operation of the computing device;

and a processor that is configured to perform, based on the determining, the one or more operations.

In another implementation, a computer-implemented method can include determining a location of a mobile computing device using one or more of a plurality of data sources; identifying a plurality of candidate responders; automatically selecting a particular candidate responder based, at least in part, on one or more factors including the availability of the candidate responders; and initiating two-way audiovisual teleconferencing between the mobile computing device and the selected particular candidate responder over a network connection.

The method can optionally include one or more of the following features. The method can further include determining or receiving a geographic location for a user; identifying, using a database of locations and corresponding responders, one or more appropriate responders based, at least in part, on the geographic location; receiving a request to connect the mobile computing device with a responder service; identifying an appropriate responder service based on the location of the mobile computing device; and initiating contact with the appropriate responder service on behalf of the mobile computing device. The method can further include receiving a geographic location for a user; and determining, using a database of locations and corresponding licensure status, whether the user is located within one or more licensed jurisdictions. The method can also include receiving, at the mobile computing device, a location of a responder through a network connection; and displaying the location of the responder on the mobile computing device. The method can additionally include establishing, before initiating a communication session at a computing device, a plurality of network connections relating to a plurality of other devices associated with candidate responders; and obtaining and displaying, using the network connections, current status information for said plurality of other devices associated with candidate responders. The method can also include receiving information identifying whether responders are currently available for communication with a user of a computing device; and in response to detecting that no

responders are currently available, taking an appropriate alternate action. The method can additionally include receiving a current location for a user; and determining a current safety level for the user at the current location based on one or more factors including said location for a user.

The details of one or more implementations are depicted in the associated drawings and description thereof below. Certain implementations may provide one or more advantages. For example, the disclosed technologies can increase security, particularly personal safety, by connecting a person or group of people at risk to responders who can help. For instance, in a crime scenario the disclosed technology can be effective at stopping or averting a crime, dissuading an attacker, and/or capturing information about the attacker, situation, and/or location that will enhance emergency personnel's ability to stop, apprehend, and/or prosecute a criminal. In a medical emergency scenario, the disclosed technology can be effective at providing real time medical information, 2-way or multi-way video, and/or capturing information about the victim, situation, and/or location that will enhance emergency personnel's ability to administer emergency care. In an accident (e.g., auto accident) or lost person scenario, the disclosed technology can aid in capturing information about the location of the person and/or other information helpful in bringing about their rescue.

In another example, before initiating a security session with a responder or other user, a user can be provided with assurances that someone is readily available to help him/her by preemptively initiating connections between the user's mobile computing device and the computing devices of other user(s) before the user has requested assistance/help. The state of such preemptive connections can be part of a Ready Mode and can allow for a user to quickly engage an available responder for assistance. Users can be notified of which other users and responders are available through user interface features, such as status indicators for a group of other users and responders, which can provide assurances of a user's available and readily deployable options for assistance.

In a further example, remote control of another user's mobile computing device can help and provide assistance to the other user in a variety of contexts. For instance, in a crime scenario such another user may not be able to activate his/her mobile computing device to obtain help from a remote user/responder. Remote activation can allow for such assistance and help to be provided. In emergency scenarios, remote activation can allow for a variety of details regarding a user's location and state to be obtained, including capturing live audio and video from the user's device and including the ability to initiate or control all of the same functions that the user himself could control on his device, which may be crucial for deploying medical personnel to an appropriate location to provide assistance.

In another example, a user needing assistance can automatically be routed to a responder who is best able to assist the user with minimal input from the user. For example, multiple factors can be considered when pairing a user in need of assistance with an appropriate responder, such as proximity of responders to the user, ratings of the responders by previous users, a type of situation (e.g., emergency, crime), user profile information and preferences, current availability of responders, responder skills and training, the group of the responder (e.g. responder is member of local police, responder is responsible for a particular jurisdiction, responder is member of private security for a particular organization), and/or other factors. Based on such factors, a user can be automatically paired with a responder who is able to best assist the user, which can improve the likelihood of a positive outcome for the user.

In a further example, by automatically sending out confirmation messages to other users/responders once a user has arrived at a destination location (for example the user's home, work, or another safe location), a user's safe arrival can be confirmed to other users (for example to the user's friends or family). Additionally, the absence of such messages after a period of time when arrival by the user at a destination was expected can allow for actions to be taken to assist the user, for example to send out notification

messages to responders or friends/family, which can reduce the response time of someone helping the user and increase the likelihood of a positive result for the user.

In another example, by providing users with updated safety scores for their surroundings based on a variety of factors, many of which would not be readily apparent to users from their physical surroundings, users can be better alerted of potentially dangerous situations and can take preventative steps to avoid any harm or danger from befalling them. For example, when a user enters a geographic area that has high crime rates and within which a recent incident report was received from another user, a safety score for that user can be provided to the user or to other users (including the user's friends, family, or responders) indicating that he/she is in an unsafe location and can suggest a route to a safer location.

In a further example, the disclosed technology can aid users in sending detailed and informative text messages to appropriate emergency responder systems (e.g., a private security company, public security company, 911 / PSAP systems), which can allow for users to quickly and silently request assistance. For example, in some instances a user may not want to initiate a video chat session or phone call with an emergency responder, such as when the user is hiding from an assailant or when there is a large amount of background noise that would render video/audio interaction useless. The disclosed technology can allow users in such situations to still obtain assistance when needed.

Other features, objects, and advantages of the technology described in this document will be apparent from the description and the drawings, and from the claims.

Brief Description of the Drawings

FIG. 1 is a conceptual diagram of an example computer system for providing security features on an example mobile computing device.

FIG. 2 is a diagram of an example system for providing security features on a mobile computing device.

FIG. 3 is a flowchart depicting an example technique for assisting a user of a computing device.

FIG. 4 is a flowchart of an example technique for initiating contact between a user's device and a responder.

FIGS. 5A-F are flowcharts of an example technique for communicating between a user device and a responder device as part of a security session.

FIG. 6 is a flowchart of an example technique for facilitating auto-answer features between a user device and a responder device.

FIG. 7 is a flowchart of an example technique for providing emergency text messaging services on a user device.

FIG. 8 is a flowchart of an example technique for providing real-time crime maps and safety levels to users.

FIGS. 9A-F are screenshots of user interfaces that can be presented on computing devices.

FIG. 10 is a screenshot of a user interface that can be presented on computing devices in Ready Mode.

FIGS. 11A-E are screenshots of a user interface that can be presented on computing devices when transitioning from Ready Mode to Caller Mode and Responder Mode.

FIGS. 12A-D are screenshots of a user interface that can be presented on computing devices to initiate and participate in two-way instant messaging.

FIG. 13 is a screenshot of a user interface that can be presented on computing devices to access several security-related features.

FIG. 14 is a screenshot of a user interface that can be presented on computing devices to display and access several security-related features.

FIG. 15 is a screenshot of a user interface that can be presented on computing devices during a 2-way video chat.

FIG. 16 is a screenshot of a user interface that can be presented on computing devices to display and access several security-related features.

FIG. 17 is a screenshot of a user interface that can be presented on computing devices to report an incident.

FIGS. 18A-B are a screenshot of a user interface through which a user can enter their profile information and register to use the security features discussed above.

FIG. 19 is a screenshot of a user interface that depicts a safety level indicators.

FIG. 20 is a screenshot of an example home screen for a mobile security application.

FIG. 21 is a screenshot of an example user interface through which a user can enter and transmit a text message to emergency responders.

Definitions

Substantially Immediate/Substantially Immediately, as used herein, refers to a short period of time between process steps. For example, if one process follows another preceding processes substantially immediately, the following occurs within a time period of less than X seconds, such as within a period of time less than X=300, 60, 30, 10, 5, 4, 2, 1, 0.5, 0.2, 0.1, 0.01, 0.001, 0.0001, 0.00001, 0.000001 seconds or less. Live connection or live video may mean video that is seen by the remote peer substantially immediately relative to the time that it is captured (e.g., when a single frame is capture by a caller, it is seen within 300, 60, 30, 10, 5, 4, 2, 1, 0.5, 0.2, 0.1, 0.01, 0.001, 0.0001, 0.00001, 0.000001 seconds or less by the responder). In Ready Mode, available instantly may mean that a live connection may be established substantially immediately.

Substantially real time, as used herein, refers to a short period of time between process steps. For example, something occurs in substantially real time if it occurs within a time period of less than X seconds, such as within a time period of less than X=300,60,30, 10,5, 4, 2, 1, 0.5, 0.2, 0.1, 0.01, 0.001, 0.0001, 0.00001, 0.000001 seconds or less.

Detailed Description

This document generally describes computer-based technology for providing security features that are readily accessible to users of computing devices, such as mobile

computing devices. A variety of different security features are described below with regard to the figures.

FIG. 1 is a conceptual diagram of an example computer system 100 for providing security features on an example mobile computing device 102. In particular, in the depicted example the mobile computing device 102 enters Ready Mode through preemptive communication with one or more other computing devices 108a-d and initiates a video communication session with one or more of the other computing devices while simultaneously transmitting video and other data to a remote data storage system 106 for secure storage 130.

The depicted computer system 100 includes the mobile computing device 102 that communicates over a network 104 with a data storage computer system 106 and a plurality of other computing devices 108a-d. The mobile computing device 102 can be any of a variety of appropriate mobile computing device, such as a smartphone, a PDA, a tablet computing device, a laptop, a wearable computing device (e.g., GOOGLE GLASS, smartwatches), a computing device embedded within a vehicle (e.g., embedded automobile computer system, truck, car, airplane, bus, helicopter, boat), and/or other appropriate mobile computing device. In some implementations, the mobile computing device 102 can be a non-mobile computing device, such as a desktop computer.

The network 104 can be any of a variety of appropriate networks over which the mobile computing device 102 can communicate with the data storage computer system 106 and/or the other computing devices 108a-d, such as the internet, local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), mobile data networks (e.g., 4G wireless networks), wireless networks (e.g., Wi-Fi networks, BLUETOOTH networks), peer-to-peer connections, TCP/IP, UDP, secure networks such as HTTPS, or any combination thereof.

The data storage computer system 106 can be any of a variety of appropriate computer system with associated storage devices, such as cloud-based computer systems with

associated data storage subsystems. The other computing devices 108a-d can be any of a variety of appropriate computing device and/or computer system, such as mobile computing devices, desktop computers, and/or computer servers.

As depicted in FIG. 1, the mobile computing device 102 is associated with a user 110 who is faced with a possible dangerous situation or person 112, which can include any of a variety of dangers or emergencies such as another person (e.g., aggressor, criminal), a medical emergency, an accident (e.g., automobile accident), and/or other dangerous physical situations.

Even before the user 110 is faced with the possible danger 112, the mobile computing device 102 can preemptively establish connections with the data storage system 106 and/or some or all of the other computing devices 108a-d over the network 104, as indicated by step A (114). These preemptive connections can be part of Ready Mode, which the user 110 may toggle on/off through one or more settings on the mobile computing device 102. As part of Ready Mode, the mobile computing device 102 periodically (e.g., every second, every 5 seconds, every 10 seconds) provides to and receives status information (e.g., active, inactive, user presently interacting with the mobile computing device 102) from to the other devices 106 and 108a-d. This status information can indicate whether a user/service associated with a corresponding device is presently available to participate in a security session. For example, status information for the data storage system 106 can indicate whether recording of information obtained by the mobile computing device 102 (e.g., video, audio, location information, sensor data) can be instantly initiated (e.g., initiated with less than a threshold delay) by the data storage system 106.

Each of the other computing devices 108a-d can be associated with one or more different entities, such as the example entities depicted in FIG. 1. For example, the computing device 108a is depicted as being associated with acquaintances 116a (e.g., friends, colleagues, family members) of the user 110, the computing device 108b is depicted as being associated with a professional security service 116b (e.g., non-government

groups/companies that provide security services), the computing device 108c as being associated with an emergency response system 116c (e.g., 911 / PSAP system), and the computing device 108d is depicted as being associated with emergency responders 116d (e.g., police officers, fire fighters, emergency medical service providers, military).

Through the preemptively established connections with these devices 108a-d, status information for users associated with the entities 116a-d can be obtained. The status information can indicate any of a variety of details regarding the availability of the computing devices 108a-d and/or associated entity users 116a-d to participate in a security session with the user 110 and the mobile computing device 102. For example, the status information can indicate whether users are currently at or away from the computing device 108a-d, which can be determined by the computing devices 108a-d based on any of a variety of information, such as whether the users are currently providing input to the computing devices 108a-d (e.g., typing, clicking on screen elements, having an app in the foreground of the device, moving a pointer device) and/or whether the users are visible through a camera of the computing devices 108a-d. In another example, the status information may include a current video feed from the computing devices 108a-d so that the user 110 can verify whether the users for entities 116a-d are currently available to provide assistance. Such a video feed may be provided at a lower level of quality (e.g., lower frame rate, lower resolution) than typically provided during video chat sessions, so as to minimize the bandwidth consumed from the transmission. In another example, the status information may include the person's location or distance from the user.

The mobile computing device 102, during Ready Mode, can display information that identifies the available entities and status information for them, as indicated by step B (118). For example, the mobile computing device 102 can display a map that includes icons identifying the location of the computing devices 108a-d and their associated users 116a-d relative to a location of the mobile computing device 102, as well as their current status information. These icons may include photos of the associated users, when they

were last connected, when they last changed position, or their computed safety level or other information. In another example, the mobile computing device 102 can display a list of the computing devices 108a-d, their corresponding users 116a-d, and their corresponding status information. In another example, the mobile computing device 102 can present a preview of a video that would be provided to the data storage system 106 for recordation along with an indicator (e.g., blinking light/icon) as to whether the data storage system 106 is available to instantaneously begin recordation of such data, and whether such recording has started or is ongoing. In some implementations, when no entities are available for the user 110, the mobile computing device can provide a notification that no responders are available to help and can additionally provide one or more alternative channels of assistance, such as dialing emergency response services (e.g., 911 service, campus police).

The information regarding the computing devices 108a-d and their corresponding entities 116a-d can be presented in a selectable manner on the mobile computing device 102 such that the user 110 can select one or more of the entities 116a-d for a security session (e.g., video communication and data recordation at the data storage system 106) or other communication session (e.g., messaging communication system).

The mobile computing device 102 can monitor for and detect input that indicates an intention of the user 110 to initiate a security session, as indicated by step C (120). Such input can take any of a variety of forms. For example, a user can select a graphical user interface feature (e.g., icon, virtual button) or physical button on the mobile computing device 102, or on another device connected to the mobile computing device 102 by wired or wireless connection (e.g., wearing watch or piece of jewelry with an embedded button to activate the app), provide audible input (e.g., utter a particular phrase), and/or provide motion based input (e.g., shaking the device) that is associated with initiating a security session. In another example, the absence of input for a period of time may indicate such an intention (e.g., holding the device in a particular orientation and/or pose for at least a threshold period of time, pressing a button down for at least a threshold period of time

before releasing it). In another example, detected motion that is indicative of the user 110 losing control of the device 102 (e.g., dropping the device 102) and/or being involved in a physical altercation (e.g., automobile accident, physical scuffle) can be identified by the mobile computing device 102 as input to initiate a security session. In another example, detected motion such as a change in velocity (for example when a car abruptly stops, potentially indicating an accident) can be identified by the mobile computing device 102 as input to initiate a security session.

In response to detecting the input, the mobile computing device 102 can automatically initiate a security session with one or more of the computing devices 108a-d and the data storage system 106, as indicated by step D (122). In instances where the user 110 has not selected one of the computing devices 108a-d to communicate with, the mobile computing device 102 itself can automatically select one or more of the computing devices 108a-d with which to initiate the security session based on a variety of factors, such as proximity to the mobile computing device 102, ratings associated with the corresponding entities 116a-d, expertise and skills for the corresponding entities 116a-d, an indication of the type of possible danger 112, predefined preferences for the user 110, one or more lists/rankings of entities 116a-d as designated by the user 102, presence within one or more emergency response jurisdictions, sensor data, or any combination thereof. Other appropriate factors can also be used. In other words, if the user is associated with a whole group of potential connection recipients, for example a whole group of potential responders, the device 102 can automatically select an appropriate potential connection recipient based on a number of factors such as proximity to the user, and initiate a connection.

As part of the security session, the mobile computing device 102 can concurrently transmit audio, video and other data to the data storage system 106, as indicated by step E (124), and can participate in a video communication session with one or more of the computing devices 108a-d, as indicated by step F (126), potentially simultaneously. The data storage system 106 can receive a stream of real-time audio, video and other data

(e.g., location information, sensor data, identity of other computing devices located nearby the mobile computing device 102), and can store the data, as indicated by step G (128). The data can be stored in one or more secure storage devices 130 to which access is restricted. For example, the data can be encrypted and stored in the secure storage devices 130, and read/write/delete privileges can be restricted such that, other than administrators of the data storage system 106, no users are able to modify the data written to the secure storage devices 130. For instance, the user 110 is not able to delete data that is uploaded to the data storage system 106 and stored in the secure storage devices 130.

The data stored in the secure storage devices 130 can be stored in a manner that will permit for the data to be used as evidence, sufficient for admission before a judicial or administrative body, of events that took place between the user 110 and the possible danger 112. As such, the data storage system 106 may trace and record information regarding a communication route over the network 104 between the mobile computing device 102 and the data storage system 106, as indicated by step H (131). Additionally, the data storage system 106 may also obtain and store raw data from the mobile computing device 102, such as raw GPS data and/or raw sensor data (e.g., motion sensor data), in addition to synthesized information from the mobile computing device 102 (e.g., geographic location determined by the mobile computing device 102). The secure storage devices 130 can store a variety of pertinent data from the mobile computing device 102, such as video/audio files, images, trace routes, location data, sensor data, and/or other appropriate data. The data being transmitted may also allow secure communication and encryption of data, as well as verification of the user transmitting the data, and the time and location from where it was transmitted. For example, the data being transmitted can be encrypted along with a username, password, time, location, biometrics, public or private cryptographic key, other security identifiers, or other information. This information may also be encrypted and or stored for verification using a blockchain-based methodology or other approaches derived from cryptography and cryptocurrencies (e.g. bitcoin, etherium). The information being transmitted can be

encrypted or stored to be only accessible or readable to the user himself, or to someone with appropriate security information. The privacy of the user, or the user's identity, can also be secured and maintained cryptographically. These encryption steps may be performed locally on the mobile device of the user. These encryption steps may be performed on the responder device. These encryption steps may be performed on a remote server.

During the established video communication session, the mobile computing device 102 can transmit, to one or more of the devices 108a-d, real-time video, audio, text or message information, and/or image data, as well as location updates, information identifying the mobile computing device 102 and/or the user 110, information that may identify another user who may be causing the possible dangerous situation (e.g., images, audio, video of the other user; detected other computing devices that are located near mobile computing device 102), and/or other appropriate information. Each of the computing devices 108a-d can additionally provide similar information to the mobile computing device 102. The information may be transmitted between the mobile computing device 102 and multiple devices from the computing devices 108a-d in substantially real time and/or using peer to peer or server-based connections. Video communication sessions can be between the mobile computing device 102 and multiple devices from the computing devices 108a-d. For example, the mobile computing device 102 can establish a first video communication session with one of the computing devices 108a associated with the user's acquaintances 116a and a second video communication session with the computing device 108b that is associated with the profession security service 116b.

In addition to transmitting real-time video feeds to the mobile computing device 102, each of the computing devices 108a-d may additionally initiate remote control over the mobile computing device 102 (e.g., turn on/off various subsystems of the mobile computing device 102, such as lights, speakers, camera, microphone, display), initiate a communication session with one or more other computing devices (e.g., the

acquaintance 116a can use the mobile computing device 108a to cause the mobile computing device 102 to communicate with the computing device 108c corresponding to the emergency response system 116c), and/or broadcast information from the video communication session to other users/devices (e.g., transmit current location and real-time video/audio feed to a nearby emergency responder 116d). Some of the entities 116a-d may have additional subsystems to further facilitate such assistance to the user, such as the professional security service 116b which can have access to emergency routing data 134 (e.g., information identifying an appropriate emergency response system (e.g., 911 or PSAP system or jurisdiction) to handle the user's 110 situation), user data 136 (e.g., information about the user 110, such as height, weight, name, age, appearance, address, automobile, medical conditions, preferences), and a secure data storage system 138 (e.g., storage system to log information regarding the interaction between the mobile computing device 102 and the computing devices 108a-d). Although not depicted, others of the computing devices 108a and 108c-d may either have data repositories similar to 134-138, or may have access to such information.

While the transmitting data to the data storage system 106 (step E) and participating in the video communication session (step F), the mobile computing device 102 can concurrently output the real-time audio and video received through the video communication session from the one or more of the computing devices 108a-d, as indicated by step I (140). Such outputting of the video can allow for a remote user (e.g., entities 116a-d) to virtually participate in the physical situation that is before the user 110 in an attempt to stop or mitigate the possible danger 112. For example, a person who is possibly dangerous 112 can see the video and/or hear the audio that is output on the user device 102, as indicated by video output 142, so as to provide verification that someone outside of the physical situation is monitoring and involved in the situation, as indicated by line 152 indicating that the video output 142 and the audio output 150 are presented to the possible danger 112. An example video output 142 on the display of the mobile computing device 102 is depicted as including textual information 144 identifying the remote user ("Police Officer"), a live video feed 146 that shows the remote user (police

officer), additional information 148 that the remote user has directed (e.g., through remote control) the mobile computing device to display 102. In the example, one of the other computing devices 108a-d that is participating in the video chat (video chat can be a multi-way (e.g., two-way, three-way, four-way) videoconference) can provide an image of the possible aggressor 112, which was obtained by the other computing device through the video communication session 126. The image of the possible aggressor 112 can serve as proof to the possible aggressor 112 that his image has been recorded, so as to imply that he/she is likely to get caught and should cease all aggression toward the user. Additionally, an audible message 150 can be output by the speakers of the mobile computing device 102.

For example, the user 110 can hold the mobile computing device 102 to be facing the possible aggressor 112 so that the possible aggressor 112 can see and hear the police officer (remote user) addressing him/her (for example the possible aggressor 112 can see the display 142). The police officer (remote user) can cause the mobile computing device 102, through remote device control, to present information to the possible aggressor 112, such as the textual information 144 identifying the police officer and the image 148 that provides verification that evidence of the possible aggressor 112 actions have been captured and are in the hands of the authorities. Such involvement by a remote user is likely to improve the chance of the possible dangerous situation 112 ending without anything having happened to the user 110. Examples of other actions that a remote user, like the police officer in the example, can cause the mobile computing device 102 to take include turning on/off a light source (e.g., flash) on the mobile computing device, activating an alarm on the mobile computing device (e.g., audible alarm or pre-recorded audio or voice message, for example 'Help!'), and/or displaying the location of an emergency responder who is en route to the user's location.

The disclosed operations that are described above as being performed by the mobile computing device 102, the data storage system 106, and the computing devices 108a-d, can be implemented in any of a variety of appropriate ways on the devices/systems, such

as through software (e.g., mobile device applications, operating system features), hardware (e.g., application specific integrated circuits (ASICs)), firmware, or any combination thereof.

FIG. 2 is a diagram of an example system 200 for providing security features on a mobile computing device 202. The example system 200 is depicted as including the mobile computing device 202, other mobile computing devices 204, computer systems 206 associated with professional security and/or emergency response systems, a data storage system 208, a central computer system 210, other computing devices 212 that are available to output audio or video information, a network 214, and wearable computing or monitoring devices 216. The mobile computing device 202 can be similar to the mobile computing device 102 described above with regard to FIG. 1. The other mobile computing devices 204 can be similar to the computing devices 108a and 108d described above. The computer system 206 can be similar to the computing devices 108b-c. The data storage system 208 can be similar to the data storage system 106. The network 214 can be similar to the network 104.

The mobile computing device 202 includes an input subsystem 216 and an output subsystem 218 through which input and output can be provided to users by the mobile computing device 202. The input subsystem 216 includes a touchscreen 220a (e.g., touch sensitive display, touch sensitive surface, touch sensitive housing, presence sensitive surface), keys and/or buttons 220b, microphone(s) 220c, motion sensors 220d (e.g., accelerometers, gyroscopes), cameras 220e (e.g., rear-facing camera, forward-facing camera, 3D cameras), and/or other appropriate technologies. In some implementations, the cameras 220e can additionally or alternatively detect portions of the electromagnetic spectrum that are outside of the range of visible light, such as infrared radiation. The output subsystem 218 includes a display 222a (e.g., LCD display, LED display), speakers 222b, a projector 222c, haptic devices 222d (e.g., vibration generating devices, tactile displays), light sources 222e (e.g., flash bulb, night vision or infrared energy), and/or other appropriate technologies. In some implementations, portions of the input and output

subsystems 216 and 218 can be configured to provide additional inputs and outputs on the mobile computing device 202. For instance, the speakers 222b can be configured to output ultrasonic and/or subsonic sound waves, the reverberation of which can be detected by the microphone(s) 220c to provide sonar detection capabilities. Similarly, the device may use radar or night vision capabilities.

The mobile computing device 202 additionally includes wireless transceivers 224 for communicating over one or more wireless communication technologies. For example, the wireless transceivers 224 can include one or more appropriate wireless transceivers, such as wireless radio transceivers like Wi-Fi transceivers, short-range wireless transceivers (e.g., BLUETOOTH transceivers), cellular network transceivers, NFC, and/or mobile data network transceivers (e.g., 3G/4G transceivers). The mobile computing device 202 can additionally include a location module 226 that is programmed to determine a location of the mobile computing device 202 either in terms of absolute positioning (e.g., GPS position data, latitude and longitude) or relative positioning (e.g., positioning relative to particular fixed objects or inside buildings including cellular toward, WiFi hotspots or networks, other radio networks, satellites). The location module 226 may include a GPS unit 228a that is programmed to detect GPS satellite signals and, based on the detected signals, to determine a geographic location of the mobile computing device 202. The location module 226 may also include a micro-location unit 228b that is programmed to determine the location of the mobile computing device 202 with a greater level of granularity than the GPS unit 228a and/or in situations where the GPS unit 228a is unreliable (e.g., interior locations). The micro-location unit 228a can use signals received through the wireless transceivers 224, such as signals from Wi-Fi networks and/or beacon signals, to determine either absolute or relative positioning of the mobile computing device 202.

The mobile computing device 202 additionally includes a CPU 230 (e.g., single core, dual core, quad core) that is programmed to execute instructions 232 (e.g., binaries, object code, scripts) that are stored/loaded into memory 234 (e.g., RAM, ROM). The CPU 230

can execute instructions of any of a variety of types to provide security features on the mobile computing device 202, such as executing instructions to cause the mobile computing device 202, through its component parts, to initiate a session with one or more of the other computing devices 204 and/or professional security/emergency response systems 206, while concurrently transmitting data for secure storage to the data storage system 208. The mobile computing device 202 can additionally include one or more portable power source 236 (e.g., a battery) or backup power sources, or power connections (e.g. to an outlet), or solar or other power inputs.

Although not depicted, the mobile computing device 202 can be provided with an appropriately sized holster/case/sleeve that is designed to receive and hold the mobile computing device 202. This case may hold the device in such a manner that the input and output subsystems 216 and 218, respectively, will be able to obtain information about the user's surroundings and convey information from remote users to other people located near the user while at the same time being worn by the user, so as to provide the user with hands free operation of the mobile computing device 202. For example, the holster/case/sleeve can be a lanyard type apparatus that is worn about around a user's neck and that holds the device in a steady position near a center of the user's chest. In another example, the holster/case/sleeve can include a clip or strap that allows for the device to easily be secured to clothing, bags, appendages, or other objects. In another example, the holster/case/sleeve can include a clip or strap that allows for the device to easily be secured to a surface such as the surface of a helmet worn by the user, a vehicle or vehicle windshield, bicycle, or other piece of equipment. The holster/case/sleeve can additionally include a reserve power source (e.g., additional batteries) that can extend the duration during which the mobile computing device 202 can be used before losing power.

The mobile computing device 202 can additionally include a security module 240 that is programmed to provide security features to a user of the mobile computing device 202, including both from the perspective of a user in need of assistance, such as the user 110

described above with regard to FIG. 1, as well as a user who is providing assistance, such as the acquaintances 116a. The security module 240 can provide security features similar to those described above with regard to FIG. 1, as well as additional/alternative security features. The security module 240, and its component parts, can be implemented in any of a variety of appropriate ways, such as through software that is executed by the CPU 230 (e.g., mobile device application, operating system features), hardware (e.g., ASICs), firmware, or any combination thereof.

The security module 240 can include a ready mode unit 242a that is programmed to establish and maintain network connections with other computing devices before an intent to initiate a security session has been detected as part of Ready Mode (e.g., step A (114) described above with regard to FIG. 1). The network connections with the other computing devices can be peer-to-peer connections. Such an intent to initiate a security session can be detected by the input analyzer 242b, which is configured to determine whether the user has, through an action (voluntary or involuntary) or omission (voluntary or involuntary), indicated an intent to initiate a security session (e.g., step B (120) described above with regard to FIG. 1).

The security module 240 additionally can include a remote control client 242c that is programmed to receive and process instructions from other computing devices (e.g., other mobile computing devices 204) to remotely control the mobile computing device 202. Before providing such remote access and control to information and components of the mobile computing device 202, such as control over the input and output subsystems 216, 218, the remote control client 242c can determine whether the requesting device and/or associated user have been given permission to have such access and control by checking against a set of permissions 242d. For example, a user may want to restrict users included on the permissions 242d to only close and trusted family members (e.g., spouse, parents, child) and friends (e.g., best friend).

The security module 240 can additionally include a routing module 242e that is programmed to determine an appropriate remote user and corresponding computing

device to which to route a security session for the mobile computing device 202. The routing module 242e can select an appropriate remote user/corresponding computing device based on one or more of a variety factors, such as proximity to the mobile computing device 202, user preferences (e.g., designation list of preferred responders), a type of situation (e.g., crime, medical emergency, natural disaster), and/or other appropriate factors. In some implementations, the routing module may alternatively be implemented at a remote computing device, such as the central computer system or server 210, which can receive a request to initiate a security session from the mobile computing device 202 and can select an appropriate other computing device for the session.

The security module 240 can store user information 242f, such as a user id, name, age, height, appearance, image, and/or preferences, which can be provided to other computing devices during security sessions. This information, for example a user profile, may also be stored on the central computer system or server 210. An identification module 242g of the security module 240 can additionally identify other users who are located around the mobile computing device through any of a variety of appropriate techniques, such as voice recognition, facial recognition, biometric identification (e.g., gait, proportions of body parts), and/or identification through nearby computing devices transmitting wireless signals (e.g., passive monitoring of wireless signals from nearby devices, active communication with such devices). The identification module 242g may use one or more data sources for such identifications, such as a user's photos, videos, social network information (e.g., friend lists, friend photos/videos, friend location, check-ins), and/or lists of contacts (e.g., telephone contact list, email contact list). The identification module 242g may alternatively and/or additionally be implemented on one or more other computing devices that are in communication with the mobile computing device 202, such as the central computer system 210 and/or the professional security/emergency response systems 206.

A text message subsystem 242h of the security module 240 can be programmed to automatically populate and/or route a text message to an appropriate emergency responder with minimal input from a user. For example, the text message subsystem 242h can add detailed information regarding the location of the mobile computing device 202, the surrounding environment, a type of emergency, and user identity information into a text message and can ensure that the text message is directed to an appropriate responder without direction from a user.

The security module 240 can include a user interface 242i through which users can access and use the security features provided by the security module 240. The user interface 242i can present information and receive input from a user in any of a variety of appropriate ways, such as through any and all components of the input and output subsystems 216 and 218, respectively.

The security module 240 additionally includes a security session manager 242j that is programmed to manage interactions between the mobile computing device 202 and other computing devices during sessions. In particular, the security session manager 242j includes a data capture manager 242k that is programmed to capture relevant data from the components of the input subsystem 216, the wireless transceivers 224, and/or the location module 226. The security session manager 242j additionally includes a data transmission manager 242l that is programmed to transmit a stream of, as least a portion of, the data captured by the data capture manager 242k to one or more of other computing devices (e.g., the other mobile computing devices 204, security/emergency response systems 206) and to the data storage system 208.

The mobile computing device 202 includes an input/output (I/O) interface 244 that is configured to communicate over the network 214 and with the wearable computing devices 216. The I/O interface 244 can be any of a variety of appropriate interface, such as a wired interface (e.g., Ethernet card) and/or wireless interface (e.g., wireless transceivers 224, wireless chips, and antennae).

The other mobile computing devices 204 can have any of the same features as the mobile computing device 202, but may be associated with other users (e.g., acquaintances, emergency responders).

The professional security/emergency response system 206 can include some or all of the components 216-244 of the mobile computing device 202, where appropriate, and may or may not be a mobile device. The professional security/emergency response system 206 can include additional components that may not be available on the mobile computing device 202 and/or the other mobile computing devices 204, such as emergency routing data 246 and/or user data 248. The emergency routing data 246 can correlate appropriate emergency response systems with the location of the mobile computing device 202. For example, the professional security/emergency response system 206 can perform a 'PSAP dip' to determine the correct 911 dispatch center for the location of a user who may be having an emergency. This function may be performed by using a database that allows every location to be converted into the corresponding PSAP/dispatch center, and to provide contact information for that dispatch center including phone number, email number, network id, and electronic communication identification. This function may be performed by a remote server, and may be performed using a remote API. One examples of a PSAP (Public Safety Answering Point) system is the PSAP PRO system provided by PitneyBowes.

The user data 248 can be a repository of relevant information for a user of the mobile computing device 202, such as the user information 242f (or a portion thereof).

The professional security/emergency response system 206 can additionally include a secure storage device(s) 250 to securely log data received from the mobile computing device 202 and/or transmitted to the mobile computing device 202 during a security session. Although not depicted, the mobile computing device 202 and/or the other mobile computing devices can also include secure storage device(s) to redundantly log such information as well.

The data storage system 208 can include a trace module 252 that is configured to encrypt and/or verify and/or trace communication paths between the data storage system 208 and the mobile computing device 202, so as to provide a proper foundation for admissibility of logged data as evidence during judicial and/or administrative proceedings. The data storage system 208 additionally include secure storage devices 254. These encryption steps may be performed locally on the mobile device of the user. These encryption steps may be performed on the responder device. These encryption steps may be performed on a remote server.

The central computer system 210 can be used to connect the mobile computing device 202 with other appropriate devices and systems, such as the data storage system 208, the other mobile computing devices 204, and the system 206. For example, the central computer system 210 can provide IP address information for the other mobile computing devices 204 to the mobile computing device 202, which the ready mode unit 242a can use to establish peer-to-peer connections with the other computing devices 204.

The other computing or monitoring or display devices 212 can be devices that are located near the mobile computing device 202 and that have open and accessible input or output devices (e.g., display 256 and speakers 258, camera, microphone) over which the mobile computing device 202 can stream and output information. For example, the other computing devices 212 can be televisions that have open Wi-Fi Direct access through which the mobile computing device 202 can broadcast audio and/or visual information. In another example, the other computing devices 212 can be specially designed and/or located security devices that allow for a user in distress to activate an alarm over an a wireless connection (e.g., BLUETOOTH connection). Such streaming of audio and visual information to the other computing devices 212 can help alert others in the area to the dangerous situation and can solicit their help. Streaming to such devices may be remotely controlled by a remote user, such as the users of the other mobile computing devices 204 and/or the system 206. Such other computing or monitoring or display devices 212 may also be used to record audio or video and transmit it to the network 214, the central

computer system 210, or to professional security /emergency response system 206, or mobile computing device 202.

The wearable computing devices 216 can include any of a variety of appropriate wearable computing device, such as eyewear (e.g., GOOGLE GLASS), smart watches, wearable cameras (e.g. GoPro, Looxcie) and/or wearable motion sensors or biosensors (e.g. heart monitor, breathing monitor, pulsox, EEG monitor, blood composition monitor including glucose monitor). The wearable computing devices 216 can provide information to the mobile computing device 202 regarding the surrounding physical environment and/or a stat of the user, and can additionally output information. Such inputting and outputting of information can be accomplished through sensors 260 (e.g., motion sensors), camera(s) 262, speakers 264, and/or other appropriate components.

FIG. 3 is a flowchart depicting an example technique 300 for assisting a user of a computing device. Portions of the technique 300 can be performed, in whole or in part, by any of a variety of appropriate computing devices and/or systems, such as the mobile computing device 102, the other computing devices 108a-d, the data storage computer system 106, the mobile computing device 202, the other mobile computing devices 204, the professional/emergency response system 206, and/or the data storage system 208.

As an overview, the technique 300 can include one or more of the following steps, which can be performed, in whole or in part, in any of a variety of appropriate orders:

Initiate Contact (302). Initiate audio, video, two-way or multi-way contact between the mobile computing device of a user (or plurality of users) and a plurality of responders. Such contact can be over peer-to-peer connections.

Continuous Real Time Recording and Transmission of Information from User (304). Information from the user or their situation may be transmitted in substantially real time by the mobile computing device of the user to computing devices/systems associated with the responder(s). This information may include audio/video from the user's device, photos, text messages, GPS or other localization information. All of this information may

be stored locally on the user and/or responders' devices, and/or on a remote server system (e.g., data storage system 106).

Continuous Real Time Recording and Transmission of Information from Responder(s)

(306). Information from the responder(s) may be transmitted in substantially real time by computing devices associated with the responders to a computing device associated with the user(s). This information may include audio/video from the responder's device, photos, text messages, GPS or other localization information. All of this information may be stored locally on the user and/or responders' devices, and/or on a server system (e.g., data storage system 106).

Remote Control of User's Device (308). The Responder(s), through their computing devices/systems, may remotely control the features of the user's device, for example to take high resolution photos using the user's device and have them sent, zoom, capture audio, adjust volume, turn on/off speaker or speakerphone, turn on/off lights, turn on/off alarms, initiate contact with other users, responders, and/or emergency services (e.g., 911 or other emergency services call) from the user's device. The remote control can allow the remote user any of the functions available locally to the user who is physically present with the device.

Help User (310). The Responder(s), through their computing devices/systems, may help the user, for example by communicating with the user or with a potential assailant through a display and/or speakers on the user's computing device. For example, the Responder may indicate, through the output subsystem of the user's computing device, to an assailant that they are being videotaped, that they should stop, or even that they are under arrest/being detained.

Dispatch Further Help (312). The Responder(s) may, through their computing devices/systems, dispatch additional support, such as emergency personnel or others to the location of the user as determined by their location information, which may be transmitted as coordinates or a map.

Store Incident Information (314). The information from the incident that is captured/obtained by the computing device of the user, such as all video, audio, locations, times, photos or other information may be stored, for example to apprehend or convict an assailant, determine fault, or aid in emergency medical diagnosis. Such information can be transmitted to one or more appropriate remote computer systems that can provide secure storage of the information (e.g., the data storage system 106).

Identification (316). In the case of an assailant, criminal, or other person, location or item involved in the incident, information captured/obtained by the user's computing device may be used to identify that person, location or item. For example, an image of the assailant may be compared with photo or other databases to identify who the assailant is to aid in the later capture of the assailant.

Rewards/Incentives for Finding, Capturing (318). This system, which may be publicly accessible or otherwise accessible to a people who may be interested in/able to provide assistance (e.g., friends of the user, law enforcement), may be used to provide information or incentives to support others in supporting the user (including finding the user), or in capturing an assailant or other criminal involved in the incident.

Black Box Tracking (320). This system may be used to provide information about the user's situation at a later time that has been transmitted to a remote location, such as the user's locations, battery levels, photos, audio, video recorded from the device, calls, texts, other activities that may be helpful in determining if the user is safe or in danger, and their location. This allows the system to track things other than people as well, including vehicles, pieces of equipment, cargo, perishables, medical supplies, remotely or autonomously controlled vehicles including automobiles and flying drones.

FIG. 4 is a flowchart of an example technique 400 for initiating contact between a user's device and a responder. The example technique 400 is depicted as being performed in part by a user device 402, a responder device 404, and a computer server system 406.

The example technique 400 can be performed as part of technique 300, for example, at step 302.

Initiating a session and finding a responder to connect to

One type of example use case of steps depicted in figure 4 is that the user of a device may launch a safety application on their mobile device, their location, subscription level, and responder groups may be determined, and based upon this an available responder may be selected that is most appropriate for them (for example the responder in their primary responder group who is physically closest to them, available online, and in the correct jurisdiction). Then, a connection may be established with that responder, either for 'Ready Mode' or for initiating a two-way communication session.

The user device 402 may be any of a variety of appropriate computing device, such as a mobile computing device (e.g., mobile computing device 102, mobile computing device 202). For example, the user device 402 can be a user's IPHONE running an IOS app that allows user to press a button to initiate contact via any of a variety of appropriate connection, such as WiFi, BLUETOOTH, 3G/4G, other mobile or VOIP signal to contact a responder. In another example, the user device 402 can be a user's ANDROID device running an ANDROID app that allows user to press a button to initiate contact via any of a variety of appropriate connection, such as WiFi, Bluetooth, 3G/4G, other mobile or VOIP signal to contact a responder. In a further example, the user device 402 can be a user's computer or tablet running an application that allows user to press a button to initiate contact via any of a variety of appropriate connection, such as WiFi, Bluetooth, 3G/4G, other mobile or VOIP signal to contact a responder.

The responder device 404 can be any of a variety of appropriate computing device (e.g., other computing devices 108a-d, other computing device 204), and can be similar to the user device 402. For example, the responder device 404 can be an IPHONE, an ANDROID device, a computer, or a tablet. Like the user device 402, the responder device 404 can also run an application, designed for an appropriate operating system of the responder

device 404, to initiate contact over any of a variety of appropriate connections, such as WiFi, Bluetooth, 3G/4G, other mobile or VOIP signal to contact a responder.

The computer server system 406 can be any of a variety of appropriate computing device or devices that act in a server role providing information to clients in response to requests. For example, the computer server system 406 can be an application server that provides information for an application to client devices, such as the user device 402 and the responder device 404.

The user device 402 can launch the application (408) in response to any of a variety of appropriate inputs. For example, the application may be launched on the user device 402 by a dedicated or selectable/configurable button. The application may be launched on the user device 402 by pressing a virtual button on the device screen. The application may be launched on the user device 402 by dropping or shaking the device. The application may be launched on the user device 402 remotely by someone else, such as by a user of the responder device 404. The application may be launched on the user device 402 by voice command / voice recognition. The application may be launched on the user device 402 by automatic recognition of a surrounding event or situation (e.g., face recognition, location recognition, position recognition, proximity to another device or user, distance from another device or user, entering or leaving a defined area). The application may be launched on the user device 402, which may serve a role as a primary mobile device, by communication with another associated mobile device, such as a button on a watch, necklace, or other device. This other device may communicate with the primary mobile device by wired or radio communication, such as WiFi or BLUETOOTH.

In some implementations, after the application has been launched the application can enter Ready Mode (410). Ready Mode is a mode of operation during which connections with other computing devices, such as the responder device 404, are established and available in advance of initiating contact to communicate (e.g., video chat, call) with users of the other computing devices. The connections with the other devices can be peer-to-peer connections. Ready Mode may be entered automatically after the application has

been launched or may be entered in response to user input (e.g., selection of a physical or virtual button, shaking the device) directing the application to enter Ready Mode.

Ready Mode can be initiated on the user device 402 through the following steps 411-422. Steps 411a-d can be performed to identify appropriate devices for the user device 402 to connect with as part of Ready Mode. For example, some responders may need to be licensed within the jurisdiction (e.g., city, county, state, country) where the user device 402 is located to provide assistance to the user. Accordingly, the user device 402 can determine one or more jurisdictions that is currently located within and can identify licensure requirements for such jurisdictions (411a). Such jurisdictional determination may be done through local data sources, such as jurisdictional and licensing information downloaded and maintained on the user device 402, and/or through remote data sources, such as jurisdictional and licensing information maintained and made available by the server system 406 and/or other computer systems. In another example, the user may have a predefined list of other users, such as friends, family, and/or specific emergency responders, that the user prefers to use as responders. The user device 402 can request a group of responders that are included on the user's predefined list(s) and/or responders who are licensed to assist within the user's current jurisdiction (411b). Such a request can be provided to one or more remote computer systems, such as the server system 406 and/or other computer systems.

Using the initial group of responders who satisfy one or more criteria (e.g., on the user's predefined list, able to assist within the jurisdiction) for the user device 402, the user device 402 can determine which of those responders are currently available to assist (411c). Such a determination can be made by polling the responder devices and/or by polling a remote computer system (e.g., server system 406) that maintains status information (e.g., current availability) for the responders. From the identified responders (e.g., available responders able to assist within the jurisdiction), the closest responders can be determined (411d). Such a determination can be made by obtaining location information for the responders, determining distances from their locations to the location

of the user device 402, and identifying a portions of the responders who are closest to the user device 402 (e.g., closest n responders, responders within threshold distance). The location information for the responders can be obtained by polling the responders and/or by requesting such information from a remote computer system (e.g., the server system 406). The steps 411a-d, in whole or in part, may alternatively be performed by a remote computing device, such as the server system 406, and/or may be performed in association with different steps in the technique 400, such as being performed at step 430.

To establish a peer-to-peer connection with the responder device 404 as part of Ready Mode, the user device 402 can transmit a request for the network addresses (e.g., IP addresses, local area network addresses) other computing devices associated with responders (412), such as the responder device 404. The request can be transmitted to the server system 406, which can maintain a list of the current network addresses (e.g., IP addresses) of computing devices that are using the application and services provided by the server system 406. The request can include information identifying the user device 402 and/or a user of the user device 402, such as a user id.

The server system 406 can receive the request (414) and can identify network addresses for other computing devices (416). The server system 406 may limit the network addresses that are identified to particular other computing devices, such as those that have been preselected by the user of the user device 402 as responder (e.g., family, friends), responders that are located near the user device's current location (e.g., police officers located near the user device 402, an appropriate 911 dispatch given the location of the user device 402, other users who are located with a threshold distance of the user device 402), and/or responder services (e.g., professional security services) that can manage response efforts and that can involve additional responders, such as police and other emergency responders, as needed. Once identified, the server system 406 can transmit the IP addresses to the user device 402 (418).

The user device 402 can receive the IP addresses (420) and can use them to establish Ready Mode connections with responder devices, such as the responder device 404 (422). The responder device 404 can connect with the user device 402 (424). The connection between the user device 402 and the responder device 404 can be peer-to-peer, which may be blocked by firewalls at either end of the connection. To avoid this a variety of techniques can be used, such as both sides attempting to connect to each other simultaneously (in case one side can't accept incoming connections but can make outbound connections), hole punching (e.g., UDP hole punching, TCP hole punching), and/or deploying relays (e.g., TURN servers).

The user device 402 can display (or otherwise present) the responders who are connected to the user device 402 in Ready Mode. Examples of such a display are depicted in Figures 10-11. In Ready Mode, a peer-to-peer connection is established between the user device 402 and the responder device 404, as indicated by steps 422 and 424. Thereafter, in Ready Mode the user device 402 can display the Responder continuously by live video, or may display an image of the available responder, with such video and images being transmitted from the responder device 404 to the user device 402 over the established peer-to-peer connection. This allows the user to see that the responder is available. The responder device 404 may not receive videos or images from the user device 402 and, thus, the responder may not see the user. The responder device 404 can be available to many users at once in this mode. In some implementations, the responder device 404 may receive and display the plurality of users connected to the responder in Ready Mode by live video. In some implementations, the responder device 404 can see the plurality of users connected to the responder in Ready Mode by live video while the user devices (e.g., user device 402) do not receive or display video or images of the responder.

Whether or not in Ready Mode (the user device 402 does not need to first enter Ready Mode), the user device 402 can monitor for user input to initiate contact with one or more responders. When the user device 402 receives input to initiate contact with a responder (430), who may or may not be specified through the input, the user device 402 can select

one or more responders to which the contact should be initiated (430) and can proceed to initiate contact with the selected responders (432), which can be accepted, automatically or in response to user consent, by the responder device 404 (434). The contact can include communication with a responder, such as video conferencing, audio conferencing (e.g., telephone call), and/or text messaging.

Contact can be initiated in a number of ways, such as shaking and/or dropping the user device 402 (e.g., detected through measurements by accelerometer(s)) and/or releasing contact with a virtual and/or physical button to indicate an emergency or intent to initiate contact. For example, in Ready Mode, a user may press a button (or provide input in any other appropriate way) to initiate contact with the Responder. Since the connection, which may be a peer-to-peer connection, between the user device 402 and the responder device 404 is already made through Ready Mode, a live video or audio call may be started between the user device 402 and the responder device 404 substantially immediately, for example in a fraction of a second.

Responders can be selected for contact at step 430 in any of a variety of ways. For example, any available responders can be selected for contact with the user device 402. In another example, responders can be selected based on the location of the user device 402 and the responders. For instance, contact may be initiated with the nearest available responder based upon the localization information of the responder and user device 402, which can be provided for in any of a variety of ways, such as by GPS, WiFi, cellular, or pre-defined localization information (E.g. physical address). In another example, responders can additionally be selected based on preferred responder lists that have been designated by the user of the user device 402, such as lists identifying particular family members or friends. Such lists may provide cascading lists of preferences and/or may designate particular responders for particular situations (e.g., medical emergency, crime). Other responder lists may also be used, such as dedicated lists of emergency responders that service an area where the user is located. In a further example, responders can additionally be selected based on user ratings of responders. For

instance, responders who have been rated as providing great service may be preferred and selected over other responders who have been rated as providing poor levels of service.

The contact can be made using any of a variety of appropriate protocols, such as peer-to-peer ad-hoc networks for audio or video or data communication, communication with or through a central server (e.g., the server system 406), and/or wireless communication using existing or future protocols, such as chat protocols (e.g., open system for communication in realtime protocol (OSCAR), talk to OSCAR protocol (TOC), iMessage protocol, Gadu-Gadu protocol, simple anonymous messaging protocol (SAM), ICQ protocol, internet relay chat protocol (IRC), QQ protocol, secure internet live conferencing protocol (SILC), Skype protocol, extensible messaging and presence protocol (XMPP), Microsoft notification protocol (MSNP), web real-time communication protocol (WebRTC)), voice over IP (VoIP) and video conferencing protocols (e.g., H.323, Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP), H.248 (also known as Media Gateway Control (Megaco)), Real-time Transport Protocol (RTP), Real-time Transport Control Protocol (RTCP), Secure Real-time Transport Protocol (SRTP), Session Description Protocol (SDP), Inter-Asterisk eXchange (IAX), Jingle XMPP VoIP extensions, Skype protocol, Teamspeak), messaging protocols (e.g., short messaging service (SMS), multimedia messaging service (MMS), enhanced messaging service (EMS)), and/or other appropriate communication protocols.

Contact and other functionality described here may use existing or future one-to-many, many-to-one and many-to-many connection systems, including social networks, such as FACEBOOK, TWITTER, SNAPCHAT, INSTAGRAM, WHATSAPP, VINE, email, and/or other appropriate systems.

The state of the user, friend or responder may be viewable by their peers/friends/opponent, including but not limited to whether the person is in the app (e.g., has launched the application, is currently using the application, whether the application currently has focus on the user's device), whether they are already on the

phone or on a video call or participating in text messaging, when the last time that they communicated was, what their last location was, whether they are at a designated location, and/or whether they are currently located in a safe or dangerous or other zone (e.g., using pre-defined 'geofenced' areas defined geographically or by proximity to a given location).

As part of the contact and communication between the user device 402 and the responder device 404, the user may record video of themselves or their surroundings using a plurality of cameras on their mobile device (user device 402), as depicted in FIG. 10-11. Some of the features that may be included in this mode are shown in these figures. This video may be saved locally on the user's device, may be saved to the responder's device, or may be saved to the web/internet/cloud on a fileserver.

FIGS. 5A-F are flowcharts of an example technique 500 for communicating between a user device and a responder device as part of a security session. The example technique 500 can be performed in part by the example user device 402, the example responder device 404, an example data storage system 403, an example restricted computer system 405, example other responder devices 407, an example emergency responder device 409, and example other devices 411. The example data storage system 403 is a computer system that remotely stores data transmitted by user and responder devices, and can be similar to the data storage system 106 and/or the data storage system 208. The example restricted computer system 405 can be a computer system that restricts data access to particular authorized users, such as computer systems associated with law enforcement (e.g., local police, FBI, CIA), the military (e.g., DOD, army, navy, airforce, marines), social networks (e.g., FACEBOOK, TWITTER), and/or other private companies (e.g., security companies, data aggregators). The example other responder devices 407 can be devices that are associated with additional responders who are different from the responder device 404. The example emergency responder device 409 can be associated with one or more emergency responders (e.g., police, fire fighters, EMTs) and can be a handled computing device (e.g., smartphone) or an embedded system within a mobile unit (e.g.,

car, ambulance). The example other devices 411 can be other computing devices that are available for receiving and outputting audio/visual information.

FIG. 5A depicts two-way communication between the user device 402 and the responder device 404, while concurrently securely transmitting and storing data associated with the communication at the data storage system 403. For example, FIG. 5A depicts steps for continuous real time recording and transmission of information from the user device 402, continuous real time recording and transmission of information from the responder 404, and helping the user of the user device 402, as described above with regard to steps 304, 306, and 312, respectively.

Connection, Location, Secure Two-Way Communication, Transmission and Storage of Data

Information from the user device 402 or their situation may be transmitted in substantially real time to the responder 404 (or multiple responders). This information from may include audio/video from the user's device, photos, GPS or other localization information. All of this information may be transmitted synchronously or asynchronously (with a delay). The intent may be to ensure that as much information is transmitted as possible, especially in the event that the time to transmit is limited. This information from may include audio/video from the user's device, photos, GPS or other localization information.

For example, the user device 402 determines its location (501) (e.g., determining GPS coordinates, determining micro-location), records audio and video using microphones and cameras that are part of or accessible to the user device 402 (502), obtains sensor data from one or more sensors that are part of or accessible to the user device 402 (503) (e.g., time sequenced motion sensor data), accesses data from one or more devices that are connected to the user device 402 (504) (e.g., obtain audio and/or video signals from wearable devices with cameras and/or microphones, obtain motion sensor data), and packages the obtained data (location, audio/video, sensor data, other data) for secured

and verified transmission to the responder device 404 and, concurrently, to the data storage system 403 (505).

The video can be obtained by the user device 402 using equipment capable of detecting electromagnetic radiation outside of the visible spectrum, such as infrared signal and/or other night vision technologies. Additionally, the user device 402 may include technology that is capable of detecting the presence and location of nearby physical objects, such as through sonar devices and other appropriate technologies. Depending on the situation facing the user, it may be difficult for the user to maintain a steady camera shot. The user device 402 can use image stabilization technology, both hardware and software, to produce video that will be easier for the responder to view and understand. Additionally, the user device 402 can passively obtain information regarding other devices that are located nearby that are transmitting wireless signals which may provide a lead as to the identity of the assailant. All such data, and other data not explicitly described but available or accessible to the user device 402, can be obtained, packaged, and transmitted to the responder device 404 and the data storage system 403.

The packaging of the data may be provided using means that allows for verification of a secure and validated connection or transmission path from the user to the recipient, or to online storage. For example, information transmitted between the user and responder, or recorded by the user or responder, may be encrypted using digital encryption, and may also include a custom digital watermark or timestamp or location stamp that may also use encryption to verify the identity and time of transmission of the user, responder or both. This technology may provide a means of verification of information transmission, for example for the use in verifying from when and where and what user this information was transmitted. This may be used later to verify this information for use as evidence. These encryption steps may be performed locally on the mobile device of the user. These encryption steps may be performed on the responder device. These encryption steps may be performed on a remote server.

The user device 402 can transmit the packaged data to the responder device 404 and to the data storage system 403 (506). The responder device 404 can update the presentation of information about the user based on the received data, such as displaying the received user video, audio, and data (511) and updating a display of the current location of the user device 402 (512). Additionally, the responder device 404 can store the data received from the user device 402 as well as the data obtained on and transmitted by the responder device 404 (513).

The responder device 404 can obtain and transmit similar information to what the user device 402 obtained and transmitted, which may be transmitted in substantially real time to the user device 402. This information from may include audio/video from the responder's device, photos, GPS or other localization information. For example, the responder may be displayed on the user's device, as in videoconferencing, video chat, and/or video broadcast. Also, pre-recorded audio, images, or video may be transmitted by the responder device 404 and displayed on user device 402.

For example, the responder device 404 can determine its location (507), record video and audio of the responder using cameras and microphones that are part of or connected to the responder device 404 (508), and package the data for secure and verified transmission in the same way as the packaging of the user device data (509). The responder device 404 can transmit the packaged data to the user device 402 and the data storage system 403 (510).

The user device 402 can display the video and audio of the responder (514) and update a display of the responder location, such as on a map that is displayed in conjunction with the video of the responder (516). In addition to storage by the responder device 404, the user device 402 can store the data received from the responder 404 and the data obtained and transmitted by the user device 402 (516). The video and audio of the responder that is output by user device 403 can help the user, for example by communicating with the user and/or with a potential assailant. For example, the Responder may indicate to an assailant that they are being videotaped, or even that they

are under arrest/being detained. In some implementations, the user device 402 the user and responder data can be stored on the user device 402 and/or the responder device 404, and uploaded to the data storage system 403 at a later time, such as when a reliable network connection with the data storage system 403 can be established.

Concurrently with the recording, transmission, and output of real-time information between the user device 402 and the responder device 404, the data storage device 403 can receive and store incident information pertaining to the communication between the user device 402 and the responder device 404. The information from the incident, such as all video, audio, locations, times, photos or other information may be stored, for example to apprehend or convict an assailant, determine fault, or aid in emergency medical diagnosis. As indicated by step 516, this information may be stored on the user's device 402. As indicated by step 513, the information may be stored on the responder(s)' device 404. The information may be stored to a central database on a central server, such as the data storage system 403.

For example, the data storage system 403 can receive the responder data (517) and the user data (519), and can trace the routes over which the responder data and user data are received so as to provide evidence of the chain of transmission (518, 520). The received data and any verification information that is determined or obtained, such as trace routes and timestamps, can be securely stored by the data storage system 403 (521). Such secure storage can include encryption, such as encryption performed by the user device 402 and/or the responder device 404, and/or encryption performed on the data by the data storage system 403.

The information that is stored by the data storage system 403 may be made available later to the user, their supporters/contacts, to emergency personnel, to the general public, or to others. Real time reports of the nature and location of incidents, and any other information provided by this system may be provided to those who need it. In some implementations, emergency responders or police officers carrying mobile devices running the software provided for here may receive real time alerts when an event has

taken place near them, including mapped information of its location, photo, video, audio or other information collected about the event. The responders contacted may include those closest to the site of the incident. In some implementations, users of this system may receive real time alerts of nearby incidents, or a map of incidents in their vicinity, which may be sorted or filtered by the time when the event occurred, proximity, types of event, or other factors.

The described storage, transmission and other functions may be performed with or without encryption of the information. All of the information may be owned, controlled, or password protected by the user, emergency responder, provider of this technology or others. All of the information collected by this technology may be provided in substantially real time via the web, for example provided to the user, a friend of the user, the responder, or a court. All of the information collected by this technology may be saved, and provided later via the web, for example provided to the user, a friend of the user, the responder, or a court. The control over the dissemination of this information may be given to the user.

As indicated by the arrows looping back to step 501 from step 516, to step 507 from step 513, and to 517 from step 521, the transmission, display, and storage of information across the user device 402, the responder device 404, and the data storage system 403 can be continuous during the 2-way communication between the user and the responder.

Although described as being performed in association with the two-way communication, the storage of data from the user device 402 and/or the responder device 404 at the data storage system 403 may be performed independent of the communication. For example, the user device 402 may begin transmitting data (e.g., location, video, audio, sensor data, peripheral device data) to the data storage system 403 for storage without being involved in a communication session with a responder device.

Screenshots are shown in FIGS. 11A-E, and described in greater detail below, show example screens that can be displayed to the caller (user device 402) and a responder (responder device 404) during 2-way communication sessions.

The responder device 404 can additionally perform a variety of actions in association with and during the 2-way communication with the user device 402. Such action, which are linked to by the circles A-E, can be performed alone or in any variety of combination with each other and are described with regard to FIGS. 5B-F.

For example, the responder or user may use pinch-to-zoom video on their own video or the opponent's (peer's) video. The responder or user may see a pinch-to-zoom or other map of the opponent's location, or may receive their address. The Responder may have an automatic or one-click way, through the responder device 404, of connecting with emergency responders responsible for the user, such as connecting with the closest or most appropriate 911 or emergency dispatch center to the user device 402 (e.g., using a PSAP dip procedure). This feature may also allow transmission of information to the 911 or emergency dispatch center, including all aspects of the information/communication between the responder device 404 and user device 402, including but not limited to the user's name, id, photo, video, audio, geolocation, situation, etc. The user's mapped location may be updated on the responder's device 404 in substantially real time, and may be presented to the responder using coordinates (including lat/long/elevation or others), an address or other place location identifier, the location of a previously-identified location such as home, school or a business name, or by depicting the user's name, userid or image on a map, which may be a pinch-to-zoom map.

FIG. 5B is a flowchart that depicts steps 522-530 for remote control of one or more features of the user device 402 by the responder device 404. For example, the responder, through the responder device 404, may remotely control the features of the users device 402, for example to take high resolution photos and have them sent, pan, focus, zoom, crop video/camera, capture audio, adjust volume, turn on/off speaker or speakerphone,

turn on/off lights, turn on/off alarms, initiate contact with other users, responders, or emergency services (e.g. 911 or other emergency services call) from the user's device 402.

Remote Control

An example use case is that a user may want to start audiovisual two-way communication with the mobile device of their friend (if their friend has given them permission to do so), without the friend having to interact with the friend's device. This may be useful in situations where the friend may not be able to interact with their device, for example if they are not in possession of it, or if they are restrained or incapacitated in some way. Another example use case is that a user may want to start audiovisual two-way communication with their own mobile device, for example if their device is lost, so that they can see what is near their device to try to recognize its location, or communicate with anyone nearby, or send a pre-recorded message, such as explaining the owner of the device or giving instructions to anyone who can hear.

The responder device 404 can receive input to control one or more features of the user device 402 (522). Based on the received input, the responder device 404 can obtain additional information to be output with the controlled feature on the responder device 402 (523). For example, the responder can select an audio recording to play on the user device 402 (e.g., siren, message warning assailant to leave the user alone). In another example, the responder can select an image to present on a display of the user device 402, such as zoomed in and enhanced image of the assailant's face so as to demonstrate to the assailant that their identity has been recorded by a third party monitoring the situation. The responder device 404 can transmit the control instructions and additional information to the user device 402 (524).

The user device 402 can receive the instructions and additional information (525) and can check permissions to determine whether to perform the operations instructed by the responder device 404 (526). The permissions may be predefined and/or rule based, and may be explicitly identified (e.g., preapproved list of responders with permission) or implicit (e.g., any responder that was contacted by the user device 402 can be provided

with implicit permission). If the responder device 404 is determined to have permission, the user device 402 can proceed to execute the instructions (527). For example, executing the instructions may toggle various feature on/off, such as cameras, speakers, microphones, displays, and/or lights (flashlights), and/or allow various adjustments to be made to currently enabled features, such as allowing for pin and zoom of the camera on the user's device 402 by the responder device 404. If additional information is provided by the responder device 404, it can be output by the user device 402 (528) (e.g., display image and/or play an audio file provided by the responder device 404). The user device 402 can report the status of the instructions (e.g., status of the feature that was changed) to the responder device 404 (529), which can in turn display the status information to the responder (530).

FIG. 5C is a flowchart that depicts example steps 531-541 for identifying an assailant based on information received from the user device 402. In the case of an assailant, criminal, or other person, location or item involved in the incident, information obtained by the user device 402 may be used to identify that person, location or item.

Identifying a Person or Assailant

In an example use case, photos or video of an assailant, user, or other person, landmark or object may be compared with photo or other databases to identify who/what they are. In the case of an assailant, this may be used for later capture, or this identity information or other information about the identified person may be transmitted to the user in substantially real time.

For example, information collected from the user device 402 about an assailant or other criminal suspect may be compared manually or using automatic image-recognition software against databases of images of people, including past-criminal databases, to identify the likely identity of suspects. This approach may be used with other types of information, including audio recordings (voice pattern matching), gate and movement information, other biometric information. This information may be used in combination

other information to improve accuracy. Such other information may include locations, affiliations, types of prior crimes, or other information to narrow down searches.

The responder device 404 can initiate identification of an assailant, objects, and/or a location where the user device 402 is located either automatically upon receiving data from the user device 402 or in response to input from the responder to begin such a process (531). The responder device 404 can identify features (e.g., face, proportions, size, shapes) of the unknown assailant, object/location from the data received from the user device 402, such as photos, videos, audio data, and/or nearby wireless devices (532). The responder device 402 can perform one or more identity matching operations for such features using local data sources, such as data sources that are maintained by the responder device 404 (e.g., repository of user identities) (533). The responder device 404 may additionally draw on data sources that are maintained by one or more restricted computer systems 405, such as computer system maintained by police, military, social networks, and/or private companies (534). Such other data sources can include a variety of identifying information on users, such as images, voice patterns, recent/current location information, and/or proportion information.

For example, in addition to having user profile information (e.g., name, address, telephone number, registered vehicles) the entity associated with the restricted computer system 405 may obtain consent from users to receive and use current location information for the users. For instance, car insurance companies offer the possibility of discounts to their customers in exchange for constantly tracking the location of their car. In another example, users frequently offer their location information to social networks as a way of notifying others of their location and/or receiving rewards. Government entities track the location of criminals through the use of monitoring bracelets, which can be offered and used as a way for released criminals to prove that they were not involved in a new crime for which they may be suspect based on their time sequenced location data. The restricted computer system 405 can obtain such user location updates (536)

and can accordingly update its database (537), which the responder device 404 can be provided with access to (535) to perform its identity matching.

Based on the identity matching, the responder device 404 can determine one or more candidate identities for the assailant/object/location (538), which can be transmitted to the user device 402 (539) and stored locally on the responder device 404 (541). The user device 402 can receive the identity information and can present/display it to the user and/or assailant (540). For example, the user device 402 can receive the identity of the assailant and can announce the name of the identified assailant as well as the assailant's address and telephone number. Such information can be persuasive in convincing an assailant that they are not going to get away with a crime against the user if one is perpetrated, and can accordingly act as a deterrent from such action and provide security to the user.

FIG. 5D is a flowchart that depicts example steps 542-550 for remotely helping the user device 402 initiate and establish a connection with another device 407.

Initiating Communication Between Other Parties

In an example use case, the responder device 404 can make a communication connection between the user device 402 and a safety responder's device (example other device 407), so that communication begins between the user and the safety responder. This communication connection may include an audio call, video call, instant messaging session. All of these may take place within a dedicated app, or may take place using standard infrastructure (e.g. third party phone lines, SMS connection, videoconferencing capability). For example, if person A receives an alert message that their friend person B may be in trouble, person A can directly initiate communication between person B and safety responder R, including without person B or responder R performing any additional action.

In another example, the responder device 404 can make a communication connection between the user device 402 and a device (other device 407) of one of the user's friends,

so that communication begins between the user of user device 402 and the friend of that user. This may take place even though the responder may not have direct knowledge of who the friend of the user that they are forming the connection to is. For example, the responder may send out a message or connection request to all of the friends who the user of user device 402 has previously selected, even though the user of user device 402 may not have direct access or knowledge of this list. This communication connection may include an audio call, video call, instant messaging session. All of these may take place within a dedicated app, or may take place using standard infrastructure (e.g. third party phone lines, SMS connection, videoconferencing capability).

In another example, the responder 404 can perform any of the other functions provided here on the user device 402. Some of these include: reporting an incident, taking a photo, uploading text, a photo, audio or video to the cloud (including using encryption based on the user device 402's encryption information, the responder device 404's encryption information, or both), placing a text message from the responder device 404 to authorities (e.g. to a PSAP/911 dispatch center), connecting with one of the responder's hero (designated/preferred responders), even if the user of user device 402 does not know who this is.

The responder device 404 can receive input suggesting that the user may need help or requesting that the user device 402 connect with the other device 407, even though the identity of the other device 407 and/or a user of the other device 407 may not be known to the responder or the user of the user device 402 (542). The responder device 404 can transmit control instructions to initiate the connection to the user device 402 (543).

The user device 402 can receive the control instructions (544) and can check whether the responder device 404 is permitted to perform such an action (545). The permissions may be predefined and/or rule based, and may be explicitly identified (e.g., preapproved list of responders with permission) or implicit (e.g., any responder that was contacted by the user device 402 can be provided with implicit permission). If the responder device 404 is determined to have permission, the user device 402 can proceed to initiate the

connection with the other device (546). If the identity of the other device is not specified in the instructions from the responder device 404, the user device 402 may proceed to select an appropriate responder, similar to the techniques described above with regard to step 430 in FIG. 4. If the IP address of the other device 407 is not known, the user device 402 can automatically identify it by contacting a central server system 406, as described with regard to steps 412-420.

The other device 407 can accept the connection with the user device 402 (547) and communication between the other device 407 and the user 402 can take place, which may additionally include communication with the responder device 404 (548-550).

Of the steps 542-550 that are described as being performed by the responder device 404 can also be performed in the reverse by the user device 402, and vice versa.

FIG. 5E is a flowchart that depicts example steps 551-560 for routing the user device 402 to an appropriate emergency responder 409.

Routing Connection to An Appropriate Responder

In an example use case, identifying an appropriate emergency responder to handle a particular type of incident at a particular geographic location can be a complex issue to solve, especially when the user requesting services is not automatically routed through a public system (PSTN) to an appropriate local responder. For instance, the jurisdictions for different types of emergency responders (police, fire fighters, EMS) may not correspond to each other and may change frequently, even depending on the current day and time.

To properly handle and route the user device 402 to the appropriate emergency responder 409, the responder device 404 can access user profile information for a user of the user device 402 (551). Such information may be stored locally by the responder device 404, which can be a part of a professional security service with which the user of the user device 402 has established an account. Accordingly, this may save the user from having to provide all of his/her pertinent details (e.g., name, age, address, medical

conditions, appearance, contact information) and, instead, the user device 402 may simply provide his/her id (e.g., device id, user id) with the responder device 404 for retrieval of this information.

The responder device 404 can access emergency routing information, which may be maintained in an up-to-date state by the responder device 404 (552), or in a connected network or database. Such emergency routing information can include geographic boundaries for various emergency responders, rules for when these boundaries may change, and other nuanced information regarding coverage by emergency responders in various geographic locations. An example of such emergency routing information is a PSAP system. In this example, the responder may determine the correct 911 or emergency dispatch center (or PSAP) based on the physical location of the user.

The responder device 404 may additionally have access to information regarding emergency responders and their current status (e.g., working, on a call, available, offline). Such access may be limited to particular responders, such as professional security service providers which may have contracted with various emergency responders throughout a geographic region to have access to such information. The responder device 404 can access the emergency responder information (e.g., skills, training, experience, geographic locations served, previous results) and the current status information for the emergency responders (554). The emergency responders for whom this information is obtained may have been selected based on the appropriate emergency routing information.

A portion of the emergency responders that are identified and for whom status information has been obtained can be selected based on a variety of factors, such as current availability, proximity to the user of the user device 402, appropriate training, skills, and/or experience to handle the user's situation (555), and the user's membership in different responder groups, or the user's subscription status or level (for example free, paid, premium). With the appropriate emergency responder(s) selected, the responder device 404 can route information regarding the user and the incident to the emergency responder device 409 that is associated with the selected responder (555).

The emergency responder 409 can receive the information regarding the user and the incident, and can use that information to begin providing assistance to the user (556). Such assistance can include travelling to the user's location or dispatching someone to the user's location (as conveyed in the information from the responder device 404), monitoring the user's situation (can be linked to the responder's data feed from the user), and/or can initiate contact with the user device 402 (559). The user device 402 can accept such contact 560, for example, the user device 402 may auto-answer the contact request from the emergency responder 409 and/or permit access to control of features on the user's device 402 (560).

For instance, the responder device 404 may dispatch additional support, such as emergency personnel or others to the location of the user device 402 as determined by their location information, which may be transmitted as coordinates or a map. For example, the responder(s) or contacts of the user may receive a map with real time updates showing the user's location, and/or their location, and/or the location of other responder(s) or contacts involved or potentially involved in supporting the user in their situation. This may include either the pre-selected contacts of the user, or other people available for support, such as other members of a network of people using this technology who have offered to be of service.

The responder device 404 may also notify the user of the selected emergency responder 409 (557), which the user device 402 can display to the user or others nearby (558).

FIG. 5F is a flowchart that depicts example steps 561-571 for causing other devices 411 that are located near the user device 402 to audibly and/or visually output information or record or monitor information.

Engaging Nearby Devices

In an example use case, the responder device 404 can direct the other device 411 (e.g., devices with displays and speakers) to output alarms and other messages (e.g., audio and/or video recorded of the responder) to solicit help for the user of the user device 402

from people located nearby and/or to identify the assailant to others in the area. For example, if a user is in an emergency in a public or private facility with appropriate other devices 411, they can activate emergency alarm sounds or lights or recording on the other devices to enhance their safety, or the safety of others at the facility.

The responder device 404 can received input to request information regarding devices that are located nearby the user device 402 (561). The responder device 440 can transmit the request to the user device 402 (562), which can receive the request (563) and identify nearby devices through polling the devices (564). Polling of the devices can be performed on a periodic and/or continuous basis, and can be performed before the input to request information about nearby devices is received. The other devices 411 can transmit their identities (565), which can be detected by the user device 402. The user device 402 can transmit information (e.g., existence, identity, type of device) regarding the nearby device to the responder device 404 (566), which can display information regarding the nearby devices to the responder (567a). The information can additionally be stored (e.g., by the responder device 404 or other computer devices, such as the data storage system 403) (567b) and access can be provided to it as a form of evidence of what is/has happened to the user of the user device 402 (567c). The responder device 404 can receive instructions to output particular information on one or more of the nearby devices (568), which can be transmitted to the user device 402 (569).

The user device 402 can receive the instructions (570) and can transmit the instructions with the particular information to the nearby devices (571). The other devices 411 can receive and output the particular information (572).

The example technique 500 can be used in a variety of scenarios. For instance, in one example medical emergency scenario the user has a medical emergency, uses their mobile device (user device 402) to run an app provided for by the disclosed technology to connect a video session with a responder (responder device 404), and the responder may communicate with the user, view the user or their emergency situation, offer advice, dispatch medical care or other personnel, or contact others.

Assailant ScenarioIn an example assailant scenario, the user is attacked or threatened by an assailant. The user may deploy their mobile device (user device 402) to dissuade such an assailant. If the user holds up the device 402, the disclosed technology provides that the device 402 and software may take video recordings of the assailant, and may allow the assailant to see a police officer, security officer, emergency responder, or one of the user's contacts, who may communicate with the assailant. For example, the responder (using responder device 404) may say "I see you, I have recorded images and video of you, we can identify you, we know exactly where you are, and anything further that you do may be used against you in a court of law." If the responder is a police officer, they may even place the assailant under arrest or detain them until law enforcement arrives on the scene, and the responder may further indicate that running away would be resisting arrest. The app/device (user device 402, responder device 404) may also send out an emergency alert to emergency services (e.g. US 911), and may send out alerts to pre-selected contacts by any means, including SMS, email, push notification, call, satellite link, pager network, videochat or others.

Lost User ScenarioIn an example lost user scenario, if a user is lost, the device (user device 402) may be useful in finding them. For example, if the user has been running an app provided for by the disclosed technology on their mobile device (user device 402) that periodically measures their location using GPS, cell-tower-based localization, wifi-based localization, or other localization technology, this information may be stored on the users device 402, or it may be transmitted to a remote location where it is stored in a database (data storage system 403), allowing the user's last known location to be used to search for the user. In addition, if the user still has a connection, the user may use the app to initiate audio or video communication with one or more emergency responders, or with one or more of their contacts. Information may be transmitted about other aspects of the user's behavior that could indicate their status, such as their remaining battery, accelerometer data, when they last sent text messages or emails or made calls, or used their device (user device 402).

Suspicious Scenario

In an example suspicious or fearful scenario, if a user feels that they are in a suspicious or fearful scenario where they are concerned that they may be in danger, they may use this technology on their mobile device (user device 402) to record people or events in their vicinity, to signal to an emergency responder that they are concerned, to signal to their pre-selected contacts that they are concerned, and/or to provide information about their estimated location based on GPS, cell, WiFi, etc. as above. The device/software (user device 402) may also allow them to be in audio and/or video communication with a responder (responder device 404). The device/software (user device 402) may also allow them to automatically initiate contact after a pre-defined time if they have not cancelled. The device/software (user device 402) may also provide for them to hold down a button which, if released, initiates automatic contact or sends out an emergency signal to responders or contacts as provided for above.

Motor Vehicle Scenario

In an example motor vehicle recording scenario, this technology may be used in or around a moving vehicle to observe accidents or video record surroundings or other drivers, and this information may be logged in the device (user device 402) and/or transmitted to a remote network (data storage system 403). In the event of a user being in an accident, this information may be used in determining that an accident has occurred (accelerometer information may be particularly useful in measuring their velocity/acceleration to determine that there was an accident), determining the user's location, determining the user's situation, and determining fault in an accident (e.g. using video of the user's vehicle and other vehicles). The device (user device 402) may be mounted to the users' dashboard, windshield, mirror, bumpers, roof, or other location chosen to facilitate recording. This information may be used to call remote assistance for the user, either automatically or by a human responder. This may be used in connection with any type of vehicle, including automobile, truck, military vehicle, boat, airplane, spacecraft, bicycle, train, bus, public transit, automatic vehicle. The device may also interface wirelessly or by wired connection with other onboard computers and sensors of

the vehicle, including cameras, pressure sensors, temperature sensors, vibration sensors, electrical sensors and others and may transmit any of this information to a remote server (where it may be recorded), or a responder in communication with the user. This may be useful in determining the situation of the user in an emergency, assisting the user, or for later use as evidence.

FIG. 6 is a flowchart of an example technique 600 for facilitating auto-answer features between a user device 402 and a responder device 404.

Auto Answer or Auto Connect

For example, the technique 600 allows the responder device 404 (which may be associated with a user, emergency responder, professional security service) to place a call to the user device 402 in such a way that the user device 402 automatically answers the call, even without the user's further action. For example, the responder device 404 may place a videocall from the responder device 404 (e.g., mobile phone) to user device 402 (e.g., mobile phone). Without the user of the user device 402 taking any further action, the software on the user device 402 (e.g., phone) automatically accepts the connection from the responder device 404. This may provide that the responder device 404 can then see video input and audio input from user device 402 (e.g., phone). The responder device 404 can also transmit their own audio (e.g. speech) and video to user device 402. All of this may be recorded. This provides a means that in an emergency situation, where the user of the user device 402 may not have access to their phone, may be incapacitated, or may be unable to press a button on their phone, the responder device 404 may still initiate communication without requiring action by the user of the user device 402. In addition, this provides a means for remote control of a device that is located someplace where it is desirable to be able to automatically initiate one-way or two-way audio, video, communication, or the other aspects of this technology. For example, a device may be mounted to a wall, or inside of a vehicle, or inside of a home or business and may act as a remotely-controllable security camera. In addition, the device may make it possible to communicate by audio and/or video to the remote location. For example, if the device is

mounted to a wall as a security camera, in the event of an intrusion, the device can begin automatically recording (including using motion and sound detection), and can also automatically place a connection to a responder, and the responder can be displayed in substantially realtime on the screen of the device, control the device, and interact with any potential intruder through two-way audio and video. In this way, a security person at a remote location can remotely intervene to stop an intrusion or other crime or inappropriate action.

In workplace settings, this technology may allow for a responder to take control over a device and begin recording and two-way communication with anyone at the scene. Example use cases include the responder serving as a remote teacher or instructor, performing quality assurance or examining work, examining items at the scene such as to determine damage to items or to assess the quantity or quality of stock. This remote control technology may also be used for the responder to be involved in remote monitoring, assistance and training in a number of contexts, including repairs, medical procedures, conversations with patients, and conversations with people at the remote scene. All of this may be recorded securely to the remote server.

The responder device 404 obtains user device 402 status information, such as information indicating whether the user device is online, offline, currently being used, on a call, and/or has not been used for n minutes (602). Such status information may be obtained through communication with a central server system. The responder device 404 can additionally receive an indication as to whether the Responder has been provided auto-answer permissions for the user device 402 – meaning that the Responder is able to initiate and automatically establish calls on the user device 402 (604). Based on the indication, an auto-answer calling feature can either be activated or deactivated on the responder device 404 (606). For example, the auto-answer calling feature can be a virtual button on the responder device 404 that, when enabled, is presented and is responsive to user contact. In contrast, if the auto-answer calling feature is inactive, such a virtual button

may not be displayed or may be otherwise indicated as being inactive (e.g., presented in gray/colorless manner).

The responder device 404 can receive selection of the auto-answer feature (608) and, in response to receiving the selection, can initiate auto-answer communication with the user device 402 (610). The communication can be one or two-way audio and/or visual communication. Auto-answer communication may be different from regular communication by the virtue of metadata that is transmitted indicating that it is an auto-answer communication request.

In response to receiving the request, the user device 402 can accept the auto-answer request (612) and can, without prompting the user of the user device 402 for consent first, obtain and transmit data (e.g., audio and/or video data, location data, device state data) to the responder device 404 (614).

The responder device 404 can display data from the user device (616) and can receive input to initiate a connection for the user device 402 with another device (618). For example, the responder may determine that the user of the user device 402 has a medical emergency and he/she is unable to request help. The responder device 404 can initiate a connection between the user device 402 and another device 407, such as an emergency responder, a professional security service, and/or an emergency handling system (e.g., E911 system).

The responder device 404 can transmit instructions to the user device 402 (620), which the user device 402 can receive and use to initiate communication with the other device 407 (624, 626).

FIG. 7 is a flowchart of an example technique 700 for providing emergency text messaging services on a user device. For example, the technique 700 can facilitate fast yet detailed emergency texts to be generated by the user device 402 and routed to an appropriate emergency responder 409 through use of the responder device 404, which may be a professional security service.

Text911

The user device 402 can receive selection of an emergency text feature (702) and, in response to receiving the selection, can begin to automatically collect pertinent information for inclusion in the text message. For instance, the user device 402 can determine its current location (704), obtain an image, video, and/or audio of the user, an assailant, and/or the user's current surroundings (706), and access stored information about the user (e.g., name, date of birth, height, weight, medical conditions, emergency contact, telephone number, preferred emergency responders) (708). The user device 402 can receive user input to identify the situation and the assistance that is needed, and/or the user device 402 can receive a selection of one or more predetermined messages (e.g., textual message, video message, audio message) (710). Such input can be textual input (e.g., typing) and/or selection of one or more fields from populated menus. Such fields can include prerecorded messages (textual, verbal, visual) that have been designated by the user and/or by other users. Using the automatically obtained information and the user input information, the user device 402 can generate a text message (712). The user device 402 can also select an appropriate responder to whom the text message should be transmitted (714), which can be similar to the selection described with regard to step 430. Selection of the responder (e.g., steps 430, 714) may additionally and/or alternatively be performed by another computing device that is different from the user device 402, such as by a computer server system. With the text message generated and the recipient selected, the text message can be transmitted to the responder device 404 (716).

The responder device 404 can receive the text (718), access emergency routing information (720), and can use the emergency routing information and the information contained in the text message (e.g., location information, type of emergency) to select an appropriate emergency responder to receive the text message (722). The steps 720 and 722 can be performed in a manner similar to steps 552-554. With the emergency responder selected, salient details from the text message regarding the emergency can be routed to the emergency responder 409 (724).

The emergency responder can receive the information (726) and can respond to the incident (728), such as transmitting a text response to the user device 402, travelling to the user's location, directing others to travel to the user's location, and/or initiating a phone or video conference with the user device 402.

The responder device 404 can additionally notify the user device 402 that the emergency responder 409 has been contacted (730), such as over a response text message. The user device 402 may receive the contact information for the emergency responder 409 (732) and can initiate contact with the emergency responder 409 (734), such as over a text message, phone call, video conference, and/or security session. The emergency responder 409 can accept the contact from the user device 402 (736). Alternatively and/or additionally, the emergency responder 409 can initiate contact that is accepted by the user device 402.

FIG. 8 is a flowchart of an example technique 800 for providing real-time crime maps and safety levels to users. The example technique 800 can be performed in part by a central computer system 802 (e.g., central computer system 210, server system 406) and first, second, and third user computing devices 804-808 (e.g., mobile computing device 102, mobile computing device 202, user device 404).

Real time crime reporting, mapping, and notification

As part of incident reporting and crime map generation, users may upload information regarding incidents that they are aware of. This information may be provided to authorities, or to other users. This information may include their location (which may be determined automatically from their device, including by GPS or WiFi-based location). This information may include the type of incident, their comments, and photos, video or audio or other types of information. This report may be registered or marked automatically on a map that is visible to other users. Reports may be sent automatically to other users, or to other users near to the site of the report. In the depicted example, the first user device 804 reports an incident which is then used to provide an update to the crime map displayed on the second user device 806 and to the safety score for the

second user device 806. For instance, the first user device 804 receives an incident report entered by the user of the first user device 804 (810), which is then transmitted to the central computer system 802 (812).

The central computer system 802 receives the incident report (814). The central computer server system 802 can provide security alerts to other users based on the incident report, as indicated by steps 815a-c. For example, the computer server system 802 can identify other users to whom the incident may be relevant and/or important (815a), such as users who are currently or are likely in the future (e.g., within a threshold period of time) to be located near where the incident occurred and/or users who are part of a group of predefined users who are identified to receive such reports (e.g., emergency responders, friends of the first user). The central computer system 802 can transmit (e.g., push notification) the alert with the incident report to the identified other users (815b), which in this example includes users who are associated with the second user device 806 and the third user device 808. The second and third user devices 806, 808 can receive and display the alert/incident report, for example, as a push notification (815c).

The central computer system 802 can also use the incident report to update real-time crime map data that is maintained by the central computer system 802 and used to provide real-time crime maps and safety levels (816). The central computer system 802 uses the updated data to generate and transmit updated map data to the second user device 806, which may receive the updated data based on the second user device 806 being currently located within a threshold distance of where the incident occurred for the first user device 804 (818). The second user device 806 can receive and display the updated map (820) and can additionally provide updated information (e.g., location) regarding the second user device 806 to the central computer system 802 (822).

The central computer system 802 can receive the current information from the second user device 806 (824) and can determine an updated safety level for the second user device based, at least in part, on the updated crime map data and/or the current information from the second user device 806 (826). The safety level for a user can be

determined based on a variety of factors, such as the current location of the user, the time of day, the day of the week, crime information for the surrounding area, recent incidents in the surrounding area, an age of the user, gender, and/or information about available responders (e.g., current availability, proximity to user, time since last active on their device). The central computer system 802 can select significant factors that contributed to the magnitude of the score (e.g., high score indicating that the user is safe, low score indicating that the user is in danger) (828). For instance, a user's score may drop suddenly indicating that he/she is suddenly less safe, and the significant factors that are selected can be those that most contributed to the decline in the score. For instance, if all of a user's responders go offline around the same time, the score for the user may drop and the selected significant factor can be the absence of available responders.

The safety level may be presented on the user's device in a number of ways. The safety level may be presented as a number. The safety level may be presented as an icon. The safety level may be presented as a color. The safety level may be presented by changing the background image or background color of the screen. The safety level may be presented through text information.

The score and significant factors can be transmitted to the second user device 806 (830).

The second user device 806 can display the score and significant factors to the user of the second user device 806 (832).

The central computer system 802 can proceed to determine whether the score has dropped below one or more threshold levels that can trigger varying levels of safety procedures (834). For example, a first level may result in simply a notice to the user and a second, more serious, level may result in a broadcast to the user's responders in addition to the user. Based on the determination, safety alerts can be transmitted (836) to the second user device 806 and, in some implementations, to a third user device 808 that may have been designated by the second user 806 as a responder. The second user device 806 and the third user device 808 can display the alerts to their respective users

(838, 840). In addition, an icon may be presented for a first user on a second user device 806 and the third user device 808 showing a coded or directly represented indication of the safety level of the first user, for example a number, or a color-coded or size-coded representation of the first user's safety level that is displayed on the second user device 806 and the third user device 808.

FIGS. 9A-F are screenshots of user interfaces that can be presented on computing devices as part of the devices, systems, and techniques described above. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

FIG. 9A depicts a screen showing remote control features that can a user of the device can select to control the operation of another user's device. The example remote control features include turning a microphone on the other user's device on/off (900), increasing the volume of speakers on the other user's device (902), turning a flashlight on the other user's device on/off (904), switching the camera that is being used on the other user's device (906), taking a picture using a designated camera on the other user's device (908), enabling/disabling an idle timer on the other user's device (910), and playing an audio file on the other user's device (912).

FIG. 9B depicts a screen showing an example video chat session, which can be one way, two-way, or multi-way among a plurality of users. In the example screen, the recipient (e.g., the responder) is seeing a real time video (914) from the user's device.

FIG. 9C depicts a mobile application screen showing example user interface elements. For instance, the depicted elements include, a button to call an emergency responder (916), a "Safe Timer" button that will issue a call to a responder if not cancelled within a specified period of time (918), a "Danger" button that will call a supporter (920), a "Protectors" button that will send a beacon signal to friends and family (922), and a "Call Me" button

that will issue a request to receive a phone call within a period of time (e.g., 10 seconds, 30 seconds, 1 minute) (924).

FIG. 9D depicts a mobile application screen showing user interface elements that include an example element 926 providing localization of a user in real time.

FIG. 9E depicts a mobile app screen showing user interface elements, such as elements 928 through which the user's information can be entered and elements 930 through which protectors/responders/friends/family/contacts can be identified either from existing data sources (e.g., contacts, FACEBOOK) or entered manually.

FIG. 9F depicts a mobile app screen showing user interface elements, such as elements through which a user can enter preferences for a period of time to wait before receiving a call back (932) and before calling a police officer (934).

FIG. 9G depicts a mobile app screen showing user interface elements, such as a real-time video of another user (936).

FIG. 10 is a screenshot 1000 of a user interface that can be presented on computing devices in Ready Mode. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

The screenshot 1000 depicts a variety of user interface features, including a flashlight toggle (1002), a button to send emergency messages with user locations to a predefined list of contacts/friends (1004), a button to call emergency response (e.g., 911) from either the user phone or a remote responder (1006), a feature to adjust the video quality/resolution/frame rate (1008), a live video and/or image of an available responder,

who may be the nearest available responder or a nearest available responder from a predefined list (1010), information identifying the availability of a responder service at a premium/priced plan (1012), a button to start a call to the responder substantially immediately (1014), a responder name or ID (1016), a button to toggle the user camera (1018), a feature indicating whether the video is being recorded based on whether the light is flashing (red) or continuously (red) (1020), and a continuous video from the user's mobile camera, which may be continuously recorded on the user's device, the responder's device, and/or a remote server system (1022).

FIGS. 11A-E are screenshots of a user interface that can be presented on computing devices when transitioning from Ready Mode to Caller Mode and Responder Mode. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

Referring to FIG. 11A, from Ready Mode, a user can select the button 1100 to initiate two-way audio/video communication to enter Caller Mode.

Referring to FIG. 11B, in Caller Mode (screen seen by the caller) the name/ID of the responder/friend who was called can be displayed (1102), the responder live video can be displayed (1104) (not displayed in audio-only mode, during which a static image may be presented), a terminate connection feature is presented (1106), and self (caller) live video or video looking out at world is presented (1108).

Referring to FIG. 11C, Responder Mode (screen seen by the responder) is presented, which is entered by the caller pressing the button 1100, sending a push notification, a call request, or connecting a friend/responder. Screen 1110 is initially presented with low quality video of the caller. Using the quality feature 1112, a higher quality video of the

caller is presented in screen 1114, as depicted in FIG. 11D. A video of the user's self (responder) is presented in window 1116. In the example depicted in FIGS. 11C-D, the screenshots show the same person as the user of the mobile computing device and the responder for mere illustrative purposes and, in general, the user and the responder will be different people using different devices.

Referring to FIG. 11E, in Responder Mode with display of a map and menu, a live video of the caller is presented 1118, a menu of remote controls of the caller's device are presented (1120) (e.g., mute, change volume, take a picture which is received by the responder, play audio on the user's device, such as an alarm, verbal commands), and a map of the caller's location, through which the responder can pinch-to-zoom, view the caller's address, and a connection to local 911/emergency center can be provided (1122).

FIGS. 12A-D are screenshots of a user interface that can be presented on computing devices to initiate and participate in two-way instant messaging. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

Referring to FIG. 12A, a list of users are presented and a two-way instant messaging session can be initiated by selecting (tapping) a user entry.

Referring to FIG. 12B, a text message session is depicted with a feature 1200 through which a user can send messages with a variety of information, including userid, user name, geolocation, map, time, date, and/or text message to a peer.

Referring to FIG. 12C, features are presented through which a request for a video call can be sent, a request for an audio call can be sent, a request for a user's exact location can

be sent, or a text message to the entire list of users friends/contacts can be sent (1202), a feature for sorting friends by proximity (1204), a feature through which a friend/user can be selected for participation in instant messaging session, audio call, video call, or other form of communication (1206).

Referring to FIG. 12D, a map is depicted showing the location of friends, with pictures and name/id, based on their most recent check-in or real-time geolocation from their device (1208). Location services can be requested for a friend and people may turn on/off the ability of other users to view their location and the toggle the level of accuracy of the location being provided to other users.

FIG. 13 is a screenshot of a user interface that can be presented on computing devices to access several security-related features. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

Button 1300 accesses a "Personal Bodyguard" screen in which a real police officer, available 24/7, will be presented to address a potential attacker by live, two-way video conferencing that he (the police officer) has already permanently recorded the attacker's face and location, and has stored that information in a secure web location with the assurance that, if any crime is committed, this evidence will be used to convict the attacker.

Button 1302 accesses a "Text 911" feature through which a user of the device can send a text message to emergency responders. Button 1304 accesses a "Contact Your Hero" screen in which you can contact another user (e.g., friend, loved one, family member) by voice, videocall, and/or text, along with providing your location to that person, allowing that person to converse with people located nearby, and to record the communication

feed. Button 1306 accesses a “Personal Security Camera” feature through which video from the device will be permanently recorded on the device as well as at a remote location so that if someone were to approach a user, the user would be able to have a permanent record of what happened, even if their phone was stolen or destroyed.

FIG. 14 is a screenshot of a user interface that can be presented on computing devices to display and access several security-related features. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

Button 1400 access a “Personal Bodyguard” screen, similar to button 1300. The “Incident Reporting” feature 1402 allows a user to report an unsafe location, crime, accident, or other emergency through the system. Incidents are reported to the appropriate authorities and other users are alerted of the incident to provide notice so as to keep them safe. The “Message All Friends” feature allows for a text message, an audio call request, or a video call request to be sent to all of a user’s friends simultaneously, with the first of your friends answering the message/request being available to the user. The “Friends List” feature is a slider that shows all of a user’s friend who can be contacted and the user’s “hero,” who is a designated person who will serve as your first responder. Button 1408 is a “Personal Security Camera” feature similar to the button 1306. Friends Map 1410 is a map that displays real-time locations and status information relating to a user’s friends. The view of the map can be changed in a variety of different ways, such as through scrolling, panning, and pinch-to-zoom interactions.

FIG. 15 is a screenshot of a user interface that can be presented on computing devices during a 2-way video chat. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the

mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

The “Record to Cloud” feature allows for videos taken by a user’s computing device, such as during a call, to be recorded directly to a remote storage location (e.g., the cloud) in a secure manner (e.g., calls and data are secure and encrypted). The “Opponent Video/Audio” feature 1502 is a real-time video display over which a user can see and hear his/her friend/hero/trained responder by two-way video conferencing using any of a variety of data connections, such as WiFi and/or cellular networks.

FIG. 16 is a screenshot of a user interface that can be presented on computing devices to display and access several security-related features. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

The map 1600 can display real-time locations of a user’s friends. The “More Ways to Help” feature 1602 allows for a user to perform operations for other users (e.g., friends, family members, contacts). To access this feature, the other user that a user would like to help may need to have provided permission for the user to help the other user. For example, a user can use this feature to have a responder call the other user, send a safety message to the other user’s friends, send a call request to the other user’s friends, and/or other features. The “Auto Answer” feature 1604 allows a user, when given appropriate permissions, to initiate a video or audio call on another user’s computing device without the other user needing to first answer the call. For example, a user can start audio and/or video communication with another user’s device even if they are not able to press a key to accept the call. The “Responder Call” feature 1606 places a call directly from another user’s device (e.g., friends’ phone) to a responder so that the responder can pick up and

engage the other user. The “Contact Friend” feature allows a user to audio call, video call, send a text message, and/or send a user’s location to another user.

FIG. 17 is a screenshot of a user interface that can be presented on computing devices to report an incident. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

The “Report an Incident” feature 1702 can map the location of an incident based on the location of the computing device and/or manual location entry. The “Submit to Cloud” feature 1700 can upload information about an incident, such as the type of incident, photos, video, audio, and/or user comments. Alerts can be sent to appropriate authorities and/or other users in response to an incident being reported.

FIGS. 18A-B are a screenshot of a user interface through which a user can enter their profile information and register to use the security features discussed above.

FIG. 19 is a screenshot of a user interface that depicts a safety level indicator 1900 for the user of the computing device displaying the user interface as well as safety level indicators 1902a-d for the user’s acquaintances, who identified at their recent/current locations on the map 1904. In the depicted example, the safety levels are identified by colors, such as green (safe), yellow (moderately safe), and red (unsafe). Other scales and intermediate levels are also possible, as well as other ways of indicating differing safety levels, such as numerical scales (e.g., scale of 1-10 in which 1 is unsafe and 10 is safe), textual descriptions (e.g., words “safe” and “unsafe”), and other user interface elements to convey to a user of the computing device safety levels for the user and his/her acquaintances. As discussed above, the safety level may be determined on the user device and/or by other computing devices (e.g., central server system) based on any of a

variety of appropriate factors, such as whether the app active on their computing device (e.g., when was the last time their location updated), the current time (e.g., daytime, nighttime), whether the user is at or near one or more known safe locations (e.g., home, work, other defined positions in a user's profile), whether and how many of the user's acquaintances are available/online in the app, whether the user is currently located in a dangerous neighborhood (e.g., based on imported this crime/map data), and/or other relevant factors.

In one example use case, a user might want to see whether his/her children are safe and can do so by looking at their safety levels on the application. If anyone is red or yellow, the user can take action to find out what is going on and, possibly, assist the user through any of a variety of the features described above, such as auto-answer and remote control. In another example use case, the a user can have an alarm set on the app so that if a friend drops below a green safety level that a notification is automatically generated. The notification can prompt the user to examine the friend's status and to possibly take action to assist the friend.

A variety of additional features can be used in combination and/or alternatively to the features discussed above. For example, rewards and/or incentives can be offered and awarded for finding and/or capturing assailants identified through the technology discussed above. For example, a rewards/incentives system may be used to provide information or incentives to support others in supporting the user (including finding the user), or in capturing an assailant or other criminal involved in an incident. For example, the user may provide information and/or a reward for the capture of an assailant. For example, the user's support network/contacts may provide information and/or a reward for finding or assisting the user if they are lost or in an emergency situation. Bounties for leading to the identification and/or capture of an assailant may be made public or private (e.g., shared with a user's social network, close friends, family).

FIG. 20 is a screenshot of an example home screen for a mobile security application that includes features to send a text to 911 (2000), securely record video and/or audio to a cloud storage device (2002), view the location and status of acquaintances and/or responders (2004), select one or more acquaintances and/or responders (e.g., slider feature) (2006), contact a particular responder (2008), and view available responders (2010). These features can be static and/or dynamic. For example, the feature 2004 may show an updated map with nearby and current acquaintance/responder locations.

FIG. 21 is a screenshot of an example user interface through which a user can enter and transmit a text message to emergency responders, such as 911 emergency services. The example user interface includes a text field into which a user can type a message (2100), a button to send a text message to emergency responders (2102), a dropdown menu through which a user can select one or more predefined incident types (e.g., crime, medical emergency, accident) (2104), an interface through which a picture, video, or other media (e.g., audio file) can be captured and/or selected for transmissions (2106), a selectable feature through which a user can indicate whether police or other emergency services should be dispatched to the user's location (2108), and a selectable feature through which a user can indicate whether police or other emergency services can call the user for further details (2110). Other features can also be included in the user interface that are not depicted in this screenshot, such as depicting a map of the user's current location, which can be modified and/or annotated (e.g., add location identifiers and descriptions to map) by the user and captured for transmission to the emergency service (e.g., screenshot of the map as modified/annotated by the user); fields through which a user can select and/or enter his/her current address; and/or a button through which a user can record a voice message that is either sent as audio or as text (using speech to text) to other users.

An affiliate program may be used to provide rewards (e.g., money, credits, free services) to users who refer the service to other users who sign up. For example, users may

broadcast the service to their acquaintances on one or more social networks. Compensation may be provided beyond first level recipients of the referral. For instance, second tier acquaintances (friends of friends) who sign up may provide compensation to the original user who promoted the service, but at a lower level of compensation than for first tier acquaintances. Such tiered sharing/promoting of the service can be used to provide a user with a personal impact map that depicts the locations of people who signed up based on their referral, either directly or indirectly. Users signing up may be color coded based on the level at which they were referred by the original user (e.g., first tier referrals can be red, second tier referrals can be orange, third tier referrals can be green).

In another example, black box style tracking of a mobile device can be used to provide information about the user's situation at a later time that has been transmitted to a remote location, such as the user's locations, battery levels, photos, audio, video recorded from the device, calls, texts, other activities that may be helpful in determining if the user is safe or in danger, and their location.

In another example, particular billing and business practices can be used to charge users for this service and technology on a subscription basis. For example, users may be charged for the purchase or use of this technology, may be charged based upon connection time, recording time or volume, or number of connections, or a combination of these.

Virality, Affiliates

Users of this system may be encouraged to have their family or friends also sign up to use this service, and to download apps/software to do so. They may be provided with incentives to engage others in this service. It may be that the family or friends need software or hardware provided by this invention to most effectively support the user (for example receiving real time push notifications, map locations for the user, one-way or two-way video, etc.). This may also allow the family or friends to thereby become users

themselves. The family or friends of a user may be able to have access to the users information, or they may only have access to select information about the user, as selected by the user in their preferences, or they may only have access to the information about a user at times or circumstances selected by the user (e.g. if the user has indicated an emergency, then their contacts get access to their location or other information), or they may only have access to the information about a user at times or circumstances selected by an emergency responder (e.g. if the emergency responder has indicated an emergency, then their contacts get access to their location or other information), or they may only have access to the information about a user at times or circumstances selected by another contact or member of this service (e.g. if a selected contact or service provider has indicated an emergency, then their contacts get access to their location or other information).

Pricing

All of the services in this invention may be priced separately, or provided for free, or bundled into different plans, or service levels, or using tiered pricing, or using country-specific or location-specific pricing. In one embodiment, features requiring recording or storage of certain information may be priced at a premium. In one embodiment, features requiring a human responder may be priced at a premium. In one embodiment, users may be charged a daily, weekly, monthly or yearly subscription fee for the use of the service. In one embodiment, users may be charged a per-minute, per-hour, per-day, per-week, per-month, or per-year usage fee for using any of the technologies features. For example, a user may be charged per-minute for recording in ready mode, for having access to a responder in ready mode, or for being in communication with a responder in ready mode.

Licensure

In one embodiment, this technology may be provided as part of a licensed service, including licensing the provider as a private patrol operator, burglar alarm or other alarm company, personal emergency response service company, private security or bodyguard company, or other types of licensing in certain jurisdictions. In one embodiment, this technology may be provided as part of a licensed service, including licensing the provider company as a private patrol operator, burglar alarm or other alarm company, personal emergency response service company, private security or bodyguard company, or other types of licensing in certain jurisdictions.

Geofencing and/or location of user

In one embodiment, certain aspects of the service may be provided only when a user is in a given jurisdiction, or within another geographically-defined region (for example using geofencing) where the provider is appropriately licensed to provide this service. Examples of appropriate licensing include holding a state burglar alarm license, a private security license, or a personal emergency response system (PERS) license. In addition, in one embodiment the service selects a responder who is appropriately licensed for the jurisdiction that a user is physically located in. For example, if a user is located in the state of California, a responder is selected who is appropriately licensed to operate in the state of California. This selection of the responder may involve looking up responder licensing information for each responder in a database stored on a server, or using data on the mobile device of the responder. Responder groups may be defined that include responders licensed for certain jurisdictions, and when a user is in that certain jurisdiction, they may be connected with responders within a responder group appropriate for, or licensed in, that jurisdiction.

In one embodiment, the provision of service may be restricted to certain geographic regions where the user is located. In one embodiment, certain aspects of the service may be provided only when a user is in a given state, country, municipality, within a set

distance of a defined position, or within another geographically-defined region (for example using geofencing).

In one embodiment, the user's location, user's language or user's language-preference may be used to select a responder based in part based upon the responder's spoken language(s) or the responder(s) location.

Examples of Hardware and Software

This disclosed technology provides for a number of different hardware devices, software applications, databases, connections, and other technologies that may be used alone or in combination. These include: mobile computing devices (e.g., mobile phones, tablets, cameras including video cameras, wearable computing devices, PDA's and other current or future devices), connection hardware (e.g., devices that may communicate via any type of existing or future wired or wireless communication method, including WiFi, Cellular (3G, 4G, LTE, 5G, etc.), internet, web, Bluetooth, etc.), web devices and/or computers (e.g., computers, servers, databases, and other hardware and software, such as computers and servers that run software that communicates and/or stores the information described), networks (e.g., wired and/or wireless networks including peer-to-peer, server-client, and other network architectures), cameras and microphones (e.g., any type of camera, microphone, speaker, lights, monitor for collecting and communicating information, such as public and/or private security cameras, cameras in the immediate vicinity of the user (based on the localization of the user and the cameras) may be used to gather further information about the user, or to display it to the responder or users contacts/supporters), drones (e.g., controlled or automatic drones that may collect or transmit information, such as automatic drones that are dispatched to the location of the user to provide real time video of the situation), and/or software.

Such software can include apps running on the users device, such as apps with videochat, recording, and other functionality as described, apps running on the responders device, such as apps with videochat, recording, and other functionality as described, and/or

website for users. A website may be provided to allow users to do things including: sign-up, provide their information; and register their mobile device(s), select and contact members of their contact list, friends (including Facebook friends or contacts from other devices or social networks), family and supporters; track all new users or prospects contacted by a user, and it may track the ones contacted by them, so that the full diaspora of users contacted directly or indirectly by a single user may be determined, and statistics, locations, numbers may be presented to the user or others. This may also be used to incentivize a user to contact others, e.g. through affiliate marketing or direct sales approaches. Other measures of the spread of the technology and its virality may also be used, such as viral coefficients and social graphs. In another example, the software may be programmed to view or share information that they have recorded during prior incidents, such as audio/video, maps of their location, to view or share information recorded or shared by other users (e.g. re-sharing information), to pay or receive payment for the use of this service, or pay for calls/time or other content, to be a website for responders (e.g. a website may be provided to allow responders/supporters to do things including: sign-up, provide their information, register their mobile device(s), select and contact other users who have selected them to be supporters or responders, such as their friends, family, or members of the public, view or share information that they or users have recorded during current or prior incidents, such as audio/video, maps of their location, and/or pay or receive payment for the use of this service, or pay for calls/time or other content). The software can additionally include social network/social network apps for users/responders. These will allow users, their networks, and responders to communicate and to share information from this invention.

The disclosed technology can also be used on non-mobile computing devices, such as desktop computers, either through dedicated software, or through a web browser, or through a portal or social network app. For example, a desktop computer can be used to do things like send out a request for connection through a social network, and have the recipient click a link that starts an app (including one that is hosted remotely so that they

don't have to download it) and allows them perform the functionality discussed throughout this document. Such interaction on a desktop computer can be performed by a webapp, which can be run within a web browser, within dedicated software, and/or through social media applications (e.g., FACEBOOK app).

WebRTC, HTML5, browser and social functionality

Additional technical features that can be used to implement this technology include WebRTC, which may be adapted with specialized code for cross-platform used, and Hybrid HTML5, which can allow for access to both native and HTML5 functionality on mobile devices. Plugins of such technologies or different technologies may also be used. WebRTC may be used for secure transmission of data, audio, video, messages, including two-way videochat, audiochat, and messaging. This information may all be recorded either locally on a user's device or responder's device. This information may all be recorded simultaneously to a remote server, including by initiating an additional webRTC connection to said remote server that streams all data to the remote server simultaneously with the two-way communication between a user and a responder. WebRTC can be used with the disclosed technology to securely transfer audio, video, data, messages, locations, images. This can be done in web browsers, using HTML5, in native IOS, ANDROID, Windows Phone, or other appropriate code. Plugins can also be used, such as those for Phonegap, Titanium, and/or Intel XDK.

The disclosed technology may additionally include a personal alarm light. This alarm light may include a flashing light. In one embodiment, this may be the 'flashlight' of a mobile phone, programmed to have a repeating flash pattern. This repeating flash pattern maybe 800msec on, 200msec off duty cycle. This repeating flash pattern maybe 500,600,700,800,900,950,990 msec on, and the balance of one second off. This flash pattern may serve as an indication that a user is using the technology. For example, this flash pattern may serve as an alarm warning light.

Device Carriers and Holders

The disclosed technology may additionally be combined with physical holsters/carriers that can be used to obtain consistent recording of a user's surrounding environment for a particular use. For example, a lanyard can be used to allow for hands free recording and operation of a mobile device. In another example, a dash cam mount can be used to allow for hands free recording while operating a vehicle. These holsters/mounts can include battery extensions (back-up power sources) and the placement of a device in these units may be detected by the device, which may in turn automatically enter a particular mode of operation.

Notifications Based on User Location

The disclosed technology may additionally include providing notifications when a user arrives at a particular geographic location or area. For example, when a user arrives home at the end of the night, a notice of the user's safe arrival may be provided to one or more other users/responders. Selection and designation of such a target location for notification can be performed by a user him/herself or by another users (e.g., responder). Additional alarms may be set and triggered if the user does not arrive at his/her destination by a particular time or within a particular window of time. In response to a user not arriving at a particular location within a particular time, other users may be notified and/or may automatically be entered into a communication session (e.g., text message session, video chat) with the user.

Training, Exercises

The disclosed technology may additionally include one or more training exercises to educate users on how to properly use the technology in the event of an emergency. Such exercised may take the form of text, audio, or video. Such exercised may take the form of games, simulations, or exercises. These simulations may train the user in scenarios designed to be similar to real-world emergency scenarios, so that in the event of a real

emergency a user will already know how to react. In one example game, similar to the common game 'assassin' or 'killer', each user in a group may receive the name of another user in the group, with no users knowing who has their name. The objective of the game can be to tag the person whose name a user has by capturing a sufficiently clear and steady image or video of that user. Once that user has been tagged, then the user gets the name of the person they just tagged to be their next objective. The game can continue until there is one remaining player. The game can teach users how to properly operate the device under physically stressful and chaotic situations, which may mirror a real life scenario.

Games

In one example of a game, which may be used in training users to use this technology, augmented reality may be used to simulate situations of emergencies, crimes, or assaults. The user may use their device within the game in a similar way to which they would use their device in a real emergency situation. The user may receive a score, or feedback, based upon how well they used the device in the simulated situation. In one example of an augmented reality game the video camera of a mobile device may be used to simulate a gun (similar to the augmented reality game phonegun or a first person shooter type game), or to simulate a camera on which a user must 'catch' (by photographing or capturing on video) another user or a specified object or location.

Social Networks

This technology can be integrated with one or more social networks (e.g., FACEBOOK, TWITTER), such as for communication, status information, message broadcasting, and other features. Privacy of the users can be maintained, with access to a user's personal data and device access being restricted to only those users or user roles (e.g., fireman, police officer) that the user has explicitly designated. Additionally, the technology may not allow for a remote user to gain access to any private data that may be stored on a

user device. The communication, settings, and automatic determinations that are made by this technology can be transparent and clearly identified to users.

A link or invitation may be sent to a first user to directly initiate a communication session with a responder. This link may be sent by email, SMS/text message, social network, or other electronic means. When the responder receives the link, including whether or not they have software installed on their local machine, they may click on the link or otherwise initiate communication using software that is stored on their local device, or software that is stored remotely from them and served to them via computer network. This may include either the user or the recipient using browser or social network plugins.

Lie Detection, Other Forms of Evidence

This technology may additionally be used in conjunction with lie detection technology, such as lie detection based on physical changes and stresses, such as blood pressure changes, breathing rate changes, heart rate changes, vocal pattern changes, and/or changes in eye movements, or brain wave (EEG, HGI) or brain scanning technologies. For example, if someone is identified as a suspect in a crime or other event using the technology, this may be verified at a later time through lie detection technology. This technology may additionally be used in conjunction with other forms of evidence, for example forensic evidence, DNA evidence, digital surveillance evidence, location evidence or others. In one example, if someone is identified as a suspect in a crime or other event using the technology, this may be verified at a later time through corroboration with other forms of evidence.

Incentive Program

An incentive program can be provided to encourage participation and assistance of other users. For example, users could receive rewards (e.g., awards, badges, points, financial rewards, credits towards payment for software or use of services, credits towards payment for time using this technology) for contacting another user to inform them of

the application, for encouraging them to download or sign up for the application, or for assisting another user in need through using the application. Such rewards could be redeemed for something (e.g., travel voucher, gift card) or publicized (e.g., press release with user's consent, national/regional award for good Samaritan). For example, a user could have displayed on a webpage how many other users they have invited to use this system, or how many other users they have as 'Friends' within this system, or how many other users have selected them as a responder or to be on a responder list.

Additional Data Sources for Geotargeted Alerts

Additional and/or alternative data sources can be used to provide geotargeted alerts to users who are located within one or more relevant geographic locations. For example, data sources providing information about emergencies (e.g., national emergency monitoring system) and/or weather-related events (e.g., weather/meteorological systems) can be accessed or can push information to this system and, when an event with at least a threshold predicted or occurring level of severity is identified, users that are located inside or within a selected distance from the affected area can receive an alert (e.g., message, recorded message, push notification) to inform them of the event, and people whom they have designated (for example their friends) can also receive a notification.

This technology can also be used with prosthetic devices, such as prosthetic devices that are controlled through brain-computer interfaces (BCIs). Aspects of the device may be controlled by BCI rather than a conventional user interface such as a touch screen. For example, data from such prosthetic devices may be provided to and used by the technology described above.

Speech to Text/Text to Speech, and Translations

Where appropriate, speech to text and text to speech technology can be used to convert speech to text for transmission/presentation to other users/devices, and to convert text to speech for presentation on user devices. Speech to text and text to speech operations

can be performed locally on a user's computing device and/or remotely on one or more remote computer systems (e.g., central computer system). Additionally, translations from one language to another can be performed on speech and/or text, so as to facilitate communication between users speaking different languages. Likewise, such translations can be performed locally and/or remotely from a user computing device.

Facilitating Cross-Jurisdictional Assistance

As discussed above, the ability of a responder to assist within a particular jurisdiction based on licensure may be checked before connecting a user with that responder. Cross-jurisdictional assistance (e.g., responder outside of user's jurisdiction providing assistance through application) may be facilitated by providing a variety of features, such as through recording security sessions, providing information to emergency authorities about ongoing cross-jurisdictional assistance, providing information to a court (e.g., to get approval), providing the responder with access to an appropriate PSAP for the user, using Ready Mode, allowing the responder to be automatically selected from a list, allowing the responder to see user's location, including as it changes and during video connection, the ability to 'cancel' repeated signals from a caller, rather than contact 911 multiple times, and/or the ability to follow up with the user later/the next day.

Call Center, QA/QC

In an example use case, the disclosed technology can be used in with call center and QA/QC functionality. For example, the disclosed technology provides for a network of responders working in a call-center environment, or working remotely at dispersed locations. The technology may be used in combination with all aspects of call center technology and best practices. Some aspects are described in: Call Center Management on Fast Forward: Succeeding in the New Era of Customer Relationships (3rd Edition) by Brad Cleveland, Layne Holley and Michael Blair (May 8, 2012), included by reference.

In particular, the technology provides for: recording/archiving of the incoming and outgoing communication by each responder and for each user, rating/grading of each communication and each responder by users or by other raters, measurement of all

parameters of each call and each responder including those typically used in call centers, including average utilization, latency to answer, length of call, quality of interaction, time to dispatch services, time to determine and document nature of call, and others. For remote responders, including responders to the scene, measurement of time from when call was received until responders arrived on scene, performed their duties can be made. This measurement may include determination of time of arrival on scene using localization technology as provided.

One-to-Many, Many-to-One, Many-to-Many

In another example, the disclosed technology can be used in a variety of different communication contexts, such as one to many, many to one, and many to many communications. For example, a single user may use this technology to communicate any of the information described to a plurality of recipients, either in real time or later.

A plurality of users may use this invention to communicate any of the information described to a plurality of recipients, either in real time or later. For example, many users at an emergency scene may all be videotaping the scene from different angles. A single responder, or a team of responders, may select all of these users and see all of their information in coordination, for example on the same screen. This technology provides for selecting which users to coordinate in this way.

A single responder may use this technology to communicate any of the information described to a plurality of users, either in real time or later. For example, if many users are at the same crime scene, a single responder may use their locations to determine that they are all at the same scene, and to handle the situation in a unified way, communicating with all of the other users at the scene, or selecting all users within a fixed distance from a chosen point, and all of the other responders involved in the incident. The responders, or users, may select which other users or responders to including in one-to-many or many-to-many communication.

It is possible to use this technology for many to many communication, so that for a given group of users and responders, all information communicated by one member of the group is communicated to the others, in real time or later, so that the group may coordinate their efforts. This may take place by group audioconference or videoconference or text message or recorded audio message. This may take place by group members sending information to other members of the group for later retrieval, for example sending group messages, notifications, emails, etc.

With Other Services Including Security, Government, Emergency Responders, Military

In another example use, this technology can be used for coordination with other services including government services. For example, this technology provided here may be used in combination with other service providers. These may include:

Security companies. This technology may be used in combination with existing security services. For example, fixed security cameras can be augmented with this technology so that while someone is being monitored on a security camera, a security guard or police officer can interact with that person by one-way or two-way audio or video.

Government Emergency Call Centers. This technology may be used in combination with emergency dispatch centers (e.g. US 911 centers). Calls, information, video, audio, text messages, user location and information may be manually or automatically routed directly to a government emergency call center for further processing or dispatch of emergency personnel or other reasons.

Military Communication. This technology may be used in combination with military communication networks and in military contexts. Calls, information, video, audio, text messages, user location and information may be manually or

automatically routed directly to a military emergency network or call center for further processing or dispatch of personnel or other reasons.

Direct communication with responders. Information may be provided directly to emergency responders. For example, if an emergency signal is sent out by a user, it may go directly to the mobile device of nearby police, providing them with any important captured information, including but not limited to the location of the user having the emergency, the identifying information of the user, any video, photos, or audio about the incident, or other useful information. This may help the responders to aid a user or victim, or to apprehend a suspect. The hardware and software may automatically detect the available responders closest to or in the best position or skills to aid with the incident.

In another example, this technology may be used in war, combat, disaster and anti-terrorism situations. For example, the technology provided herein may be used in military, police, war, combat, disaster and anti-terrorism situations to provide important information in real time and aid in these situations. Information from multiple users may be coordinated by central locations, for example displaying on a centralized map where all responses or users are coming in from, and allowing communication amongst them. This technology may have application in preventing violence within the military, including preventing violence against women perpetrated by other members of the military. This technology may also be used in real or simulated military or combat environments, including in military training, or war games, including civilian combat games like paintball, laser tag or others to coordinate teams, determine locations of users, and allow single or group communication by audio, video, text message or use of the other technology features.

Demonstration of Innocence or Guilt

This technology may be used to demonstrate a user's innocence (or guilt) in a crime or other incident. For example, if a user is using this technology, and this verifies the user's location at the time of a crime as being distant from the crime scene, this may be used to establish the innocence of the user. This may be enhanced through verification technologies that ensure that the user is physically present at the same location as the mobile device that is transmitting the location, including biometrics such as a fingerprint scanner, an iris scanner, face recognition or capturing an image or video of the user. In addition, this may be enhanced through verification technologies that are physically attached to the user, such as an ankle bracelet that communicates with the device through a wireless connection and verifies that the user is at the same location as the device, and thereby verifies that the user was or was not at a crime scene.

Lite Messaging

This technology may allow a user to send a "lite" message to initiate communication with other users in a manner that does not require the other users to have a particular application installed on their computing devices – allowing users to rely on and use the participation of other users who have not installed or registered to use a particular application (e.g., mobile security app). For example, a user can send out a lite message, for example, over email, SMS, social network messaging (e.g., FACEBOOK messaging, TWITTER), with the message including a selectable feature (e.g., link) that the recipient can select to immediately begin a connection with the sending user using existing technology on the recipient user's device (e.g., connection without the recipient user having to download/install a particular application). Selection of such a link can cause the recipient's device to identify one or more compatible technologies to use to communicate with the sending device. Such lite messaging can allow for users to send messages that create such links between the two users and to be able to use the functionality very easily and without much interaction by the recipient user (e.g., able to connect with sender with no more than 1, 2, 3, 4 clicks and/or 0,1,2,3,4 entered pieces of identification or

information). In one example, a user (calling user) can send a message including a URL link through a messaging platform (email, SMS, Facebook, others) to a responder. This URL link can contain information specifying the sender, or the sender and responder, or the sender, responder. The URL link can also optionally include additional information, including information about the kind of communication being requested, the nature of the situation or topic of communication, the means of communicating, the locations of one or both users, encryption information (for example including a public key), or other information. When the responder receives this message, the responder can click on the URL link. This can bring up in the responders browser a way to communicate with the user who sent the message. For example, the responder's click's the link this can bring up on the responder's browser or on other software on their desktop, mobile device, tablet or wearable device a web page, an app, a widget, or another way for them to communicate with the calling user who sent the message. This web page, an app, a widget, or another way for them to communicate with the calling user may not require download if sufficient resources are already available on the responder's device. If sufficient resources are not available, then those resources may be provided to the responder, for example by the responder clicking on the link, for example by a website being sent to and displayed for the responder. This may not require the responder to take additional steps to install software on his device. When this web page, app, widget or way for the responder to communicate with the calling user is displayed, it can already be connected with the user who sent the message, or it can pre in a state ready to quickly form that communication connection, for example it can be pre-populated with the calling user's id or network address. The web page, app, widget or way for the responder to communicate with the calling user can display a message asking the responder if the responder would like to communicate with the calling user, or this communication can be begun automatically. If the responder selects that they do want to communicate with the calling user, then communication can be begun.

The disclosed technology may be implemented as part of a mobile personal emergency response system (PERS).

Computing devices and computer systems described in this document that may be used to implement the systems, techniques, machines, and/or apparatuses can operate as clients and/or servers, and can include one or more of a variety of appropriate computing devices, such as laptops, desktops, workstations, servers, blade servers, mainframes, mobile computing devices (e.g., PDAs, cellular telephones, smartphones, and/or other similar computing devices), computer storage devices (e.g., Universal Serial Bus (USB) flash drives, RFID storage devices, solid state hard drives, hard-disc storage devices), and/or other similar computing devices. For example, USB flash drives may store operating systems and other applications, and can include input/output components, such as wireless transmitters and/or USB connector that may be inserted into a USB port of another computing device.

Such computing devices may include one or more of the following components: processors, memory (e.g., random access memory (RAM) and/or other forms of volatile memory), storage devices (e.g., solid-state hard drive, hard disc drive, and/or other forms of non-volatile memory), high-speed interfaces connecting various components to each other (e.g., connecting one or more processors to memory and/or to high-speed expansion ports), and/or low speed interfaces connecting various components to each other (e.g., connecting one or more processors to a low speed bus and/or storage devices). Such components can be interconnected using various busses, and may be mounted across one or more motherboards that are communicatively connected to each other, or in other appropriate manners. In some implementations, computing devices can include pluralities of the components listed above, including a plurality of processors, a plurality of memories, a plurality of types of memories, a plurality of storage devices, and/or a plurality of buses. A plurality of computing devices can be connected to each other and can coordinate at least a portion of their computing

resources to perform one or more operations, such as providing a multi-processor computer system, a computer server system, and/or a cloud-based computer system.

Processors can process instructions for execution within computing devices, including instructions stored in memory and/or on storage devices. Such processing of instructions can cause various operations to be performed, including causing visual, audible, and/or haptic information to be output by one or more input/output devices, such as a display that is configured to output graphical information, such as a graphical user interface (GUI). Processors can be implemented as a chipset of chips that include separate and/or multiple analog and digital processors. Processors may be implemented using any of a number of architectures, such as a CISC (Complex Instruction Set Computers) processor architecture, a RISC (Reduced Instruction Set Computer) processor architecture, and/or a MISC (Minimal Instruction Set Computer) processor architecture. Processors may provide, for example, coordination of other components computing devices, such as control of user interfaces, applications that are run by the devices, and wireless communication by the devices.

Memory can store information within computing devices, including instructions to be executed by one or more processors. Memory can include a volatile memory unit or units, such as synchronous RAM (e.g., double data rate synchronous dynamic random access memory (DDR SDRAM), DDR2 SDRAM, DDR3 SDRAM, DDR4 SDRAM), asynchronous RAM (e.g., fast page mode dynamic RAM (FPM DRAM), extended data out DRAM (EDO DRAM)), graphics RAM (e.g., graphics DDR4 (GDDR4), GDDR5). In some implementations, memory can include a non-volatile memory unit or units (e.g., flash memory). Memory can also be another form of computer-readable medium, such as magnetic and/or optical disks.

Storage devices can be capable of providing mass storage for computing devices and can include a computer-readable medium, such as a floppy disk device, a hard disk device,

an optical disk device, a Microdrive, or a tape device, a flash memory or other similar solid state memory device, or an array of devices, including devices in a storage area network or other configurations. Computer program products can be tangibly embodied in an information carrier, such as memory, storage devices, cache memory within a processor, and/or other appropriate computer-readable medium. Computer program products may also contain instructions that, when executed by one or more computing devices, perform one or more methods or techniques, such as those described above.

High speed controllers can manage bandwidth-intensive operations for computing devices, while the low speed controllers can manage lower bandwidth-intensive operations. Such allocation of functions is exemplary only. In some implementations, a high-speed controller is coupled to memory, display 616 (e.g., through a graphics processor or accelerator), and to high-speed expansion ports, which may accept various expansion cards; and a low-speed controller is coupled to one or more storage devices and low-speed expansion ports, which may include various communication ports (e.g., USB, Bluetooth, Ethernet, wireless Ethernet) that may be coupled to one or more input/output devices, such as keyboards, pointing devices (e.g., mouse, touchpad, track ball), printers, scanners, copiers, digital cameras, microphones, displays, haptic devices, and/or networking devices such as switches and/or routers (e.g., through a network adapter).

Displays may include any of a variety of appropriate display devices, such as TFT (Thin-Film-Transistor Liquid Crystal Display) displays, OLED (Organic Light Emitting Diode) displays, touchscreen devices, presence sensing display devices, and/or other appropriate display technology. Displays can be coupled to appropriate circuitry for driving the displays to output graphical and other information to a user.

Expansion memory may also be provided and connected to computing devices through one or more expansion interfaces, which may include, for example, a SIMM (Single In Line Memory Module) card interfaces. Such expansion memory may provide extra storage space for computing devices and/or may store applications or other information that is accessible by computing devices. For example, expansion memory may include instructions to carry out and/or supplement the techniques described above, and/or may include secure information (e.g., expansion memory may include a security module and may be programmed with instructions that permit secure use on a computing device).

Computing devices may communicate wirelessly through one or more communication interfaces, which may include digital signal processing circuitry when appropriate. Communication interfaces may provide for communications under various modes or protocols, such as GSM voice calls, messaging protocols (e.g., SMS, EMS, or MMS messaging), CDMA, TDMA, PDC, WCDMA, CDMA2000, GPRS, 4G protocols (e.g., 4G LTE), and/or other appropriate protocols. Such communication may occur, for example, through one or more radio-frequency transceivers. In addition, short-range communication may occur, such as using a Bluetooth, Wi-Fi, or other such transceivers. In addition, a GPS (Global Positioning System) receiver module may provide additional navigation- and location-related wireless data to computing devices, which may be used as appropriate by applications running on computing devices.

Computing devices may also communicate audibly using one or more audio codecs, which may receive spoken information from a user and convert it to usable digital information. Such audio codecs may additionally generate audible sound for a user, such as through one or more speakers that are part of or connected to a computing device. Such sound may include sound from voice telephone calls, may include recorded sound (e.g., voice messages, music files, etc.), and may also include sound generated by applications operating on computing devices.

Various implementations of the systems, devices, and techniques described here can be realized in digital electronic circuitry, integrated circuitry, specially designed ASICs (application specific integrated circuits), computer hardware, firmware, software, and/or combinations thereof. These various implementations can include implementation in one or more computer programs that are executable and/or interpretable on a programmable system including at least one programmable processor, which may be special or general purpose, coupled to receive data and instructions from, and to transmit data and instructions to, a storage system, at least one input device, and at least one output device.

These computer programs (also known as programs, software, software applications, or code) can include machine instructions for a programmable processor, and can be implemented in a high-level procedural and/or object-oriented programming language, and/or in assembly/machine language. As used herein, the terms “machine-readable medium” “computer-readable medium” refers to any computer program product, apparatus and/or device (e.g., magnetic discs, optical disks, memory, Programmable Logic Devices (PLDs)) used to provide machine instructions and/or data to a programmable processor.

To provide for interaction with a user, the systems and techniques described here can be implemented on a computer having a display device (e.g., LCD display screen, LED display screen) for displaying information to users, a keyboard, and a pointing device (e.g., a mouse, a trackball, touchscreen) by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback (e.g., visual feedback, auditory feedback, and/or tactile feedback); and input from the user can be received in any form, including acoustic, speech, and/or tactile input.

The systems and techniques described here can be implemented in a computing system that includes a back end component (e.g., as a data server), or that includes a middleware component (e.g., an application server), or that includes a front end component (e.g., a client computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the systems and techniques described here), or any combination of such back end, middleware, or front end components. The components of the system can be interconnected by any form or medium of digital data communication (e.g., a communication network). Examples of communication networks include a local area network ("LAN"), a wide area network ("WAN"), peer-to-peer networks (having ad-hoc or static members), grid computing infrastructures, and the Internet.

The computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

The above description provides examples of some implementations. Other implementations that are not explicitly described above are also possible, such as implementations based on modifications and/or variations of the features described above. For example, the techniques described above may be implemented in different orders, with the inclusion of one or more additional steps, and/or with the exclusion of one or more of the identified steps. Additionally, the steps and techniques described above as being performed by some computing devices and/or systems may alternatively, or additionally, be performed by other computing devices and/or systems that are described above or other computing devices and/or systems that are not explicitly described. Similarly, the systems, devices, and apparatuses may include one or more additional features, may exclude one or more of the identified features, and/or include the identified features combined in a different way than presented above.

Features that are described as singular may be implemented as a plurality of such features. Likewise, features that are described as a plurality may be implemented as singular instances of such features. The drawings are intended to be illustrative and may not precisely depict some implementations. Variations in sizing, placement, shapes, angles, and/or the positioning of features relative to each other are possible.

What is claimed is:

1. A computer-implemented method comprising:
 - determining a location of a mobile computing device using one or more of a plurality of data sources;
 - communicating, by the mobile computing device, with another computing device as part of a two-way video chat session over a first network connection, the communicating including transmitting the location of the mobile computing device; and
 - displaying, as part of the two-way video chat session, real-time video from the other computing device;
 - recording video using one or more cameras that are accessible to the mobile computing device; and
 - transmitting, over a second network connection, the video to a remote storage system for persistent storage.
2. The computer-implemented method of claim 1, further comprising:
 - identifying from a data source a plurality of potential responder computing devices associated with candidate responders; and
 - automatically selecting a particular potential responder computing device to communicate with that is associated with a particular potential candidate responder based, at least in part, on one or more factors including the availability of the responder for communication.
3. The computer-implemented method of claim 1, further comprising:
 - receiving, at the mobile computing device, a location of a responder through a network connection; and
 - displaying the location of the responder on the mobile computing device.
4. The computer-implemented method of claim 1, further comprising:
 - receiving information that indicates whether responders are currently available for a user of the mobile computing device; and
 - if it is detected that no responders are currently available, taking an appropriate alternate action.

5. The computer-implemented method of claim 1, further comprising:
 - establishing, before initiating the communication session at the other computing device, network connections with a plurality of other devices associated with candidate responders; and
 - obtaining and displaying, using the network connections, current status information for a plurality of candidate responders.

6. The computer-implemented method of claim 1, further comprising:
 - receiving, at the mobile computing device and from a responder computing device, instructions to perform one or more operations;
 - determining whether the responder computing device is permitted to remotely control operation of the mobile computing device; and
 - if the responder computing device is permitted to remotely control operation of the mobile computing device based on the determining, performing, the one or more operations.

7. The computer-implemented method of claim 1, further comprising:
 - encrypting, by the mobile computing device, real-time data with associated metadata that identifies when, where, or by whom the real-time data was collected;
 - and
 - transmitting the real-time data.

8. The computer-implemented method of claim 1, further comprising:
 - receiving a current location for a user; and
 - determining a current safety level for the user at the current location based on one or more factors including the location.

9. The computer-implemented method of claim 1, wherein a communication protocol that is used comprises webRTC.

10. A computing device comprising:
 - one or more cameras that are programmed to record video;
 - a geographic location unit that is programmed to determine a location of a computing device using one or more of a plurality of data sources;
 - a network interface that is programmed to communicate with another computing device as part of a two-way video chat session over a first network connection and to cause the video to be transmitted, over a second network connection, to a remote storage system for persistent storage, the location of the computing device being sent over the first and second network connections; and
 - a display that is programmed to display, as part of the two-way video chat session, real-time video from the other computing device.

11. The computing device of claim 10, further comprising:
 - a security application that is programmed to identify a plurality of candidate responders and to select a particular candidate responder based, at least in part, on one or more factors, wherein the particular candidate responder is associated with the other computing device.

12. The computing device of claim 10, wherein the network interface is further programmed to establish, before initiating the communication with the other computing device, network connections with a plurality of other computing devices associated with candidate responders;
 - wherein the device further comprises:
 - a status module that is programmed to obtain, using the network connections, current status information for a plurality of candidate responders; and
 - wherein the display is programmed to display the current status information for a plurality of candidate responders.

13. The computing device of claim 10, wherein the network interface is further programmed to receive, from a responder computing device, instructions to perform one or more operations;
 - wherein the computing device further comprises:

a permissions module that is programmed to determine whether the responder computing device is permitted to remotely control operation of the computing device; and

a processor that is configured to perform, based on the determining, the one or more operations.

14. A computer-implemented method comprising:

determining a location of a mobile computing device using one or more of a plurality of data sources;

identifying a plurality of candidate responders;

automatically selecting a particular candidate responder based, at least in part, on one or more factors including the availability of the candidate responders; and

initiating two-way audiovisual teleconferencing between the mobile computing device and the selected particular candidate responder over a network connection.

15. The computer-implemented method of claim 14, further comprising:

determining or receiving a geographic location for a user;

identifying, using a database of locations and corresponding responders, one or more appropriate responders based, at least in part, on the geographic location;

receiving a request to connect the mobile computing device with a responder service;

identifying an appropriate responder service based on the location of the mobile computing device; and

initiating contact with the appropriate responder service on behalf of the mobile computing device.

16. The computer-implemented method of claim 14, further comprising:

receiving a geographic location for a user; and

determining, using a database of locations and corresponding licensure status, whether the user is located within one or more licensed jurisdictions.

17. The computer-implemented method of claim 14, further comprising:
 - receiving, at the mobile computing device, a location of a responder through a network connection; and
 - displaying the location of the responder on the mobile computing device.

18. The computer-implemented method of claim 14, further comprising:
 - establishing, before initiating a communication session at a computing device, a plurality of network connections relating to a plurality of other devices associated with candidate responders; and
 - obtaining and displaying, using the network connections, current status information for said plurality of other devices associated with candidate responders.

19. The computer-implemented method of claim 14, further comprising:
 - receiving information identifying whether responders are currently available for communication with a user of a computing device; and
 - in response to detecting that no responders are currently available, taking an appropriate alternate action.

20. The computer-implemented method of claim 14, further comprising:
 - receiving a current location for a user; and
 - determining a current safety level for the user at the current location based on one or more factors including said location for a user.

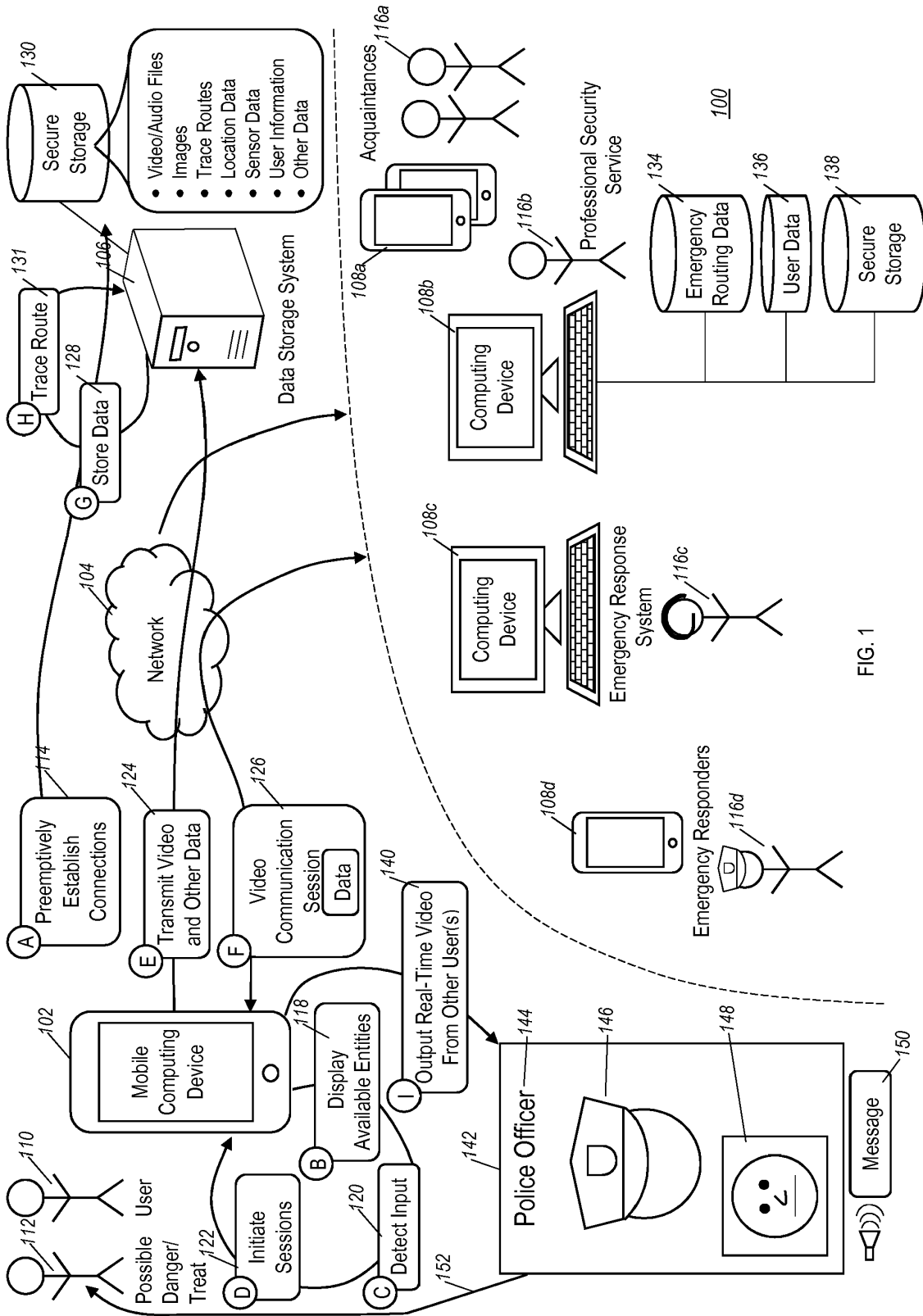


FIG. 1

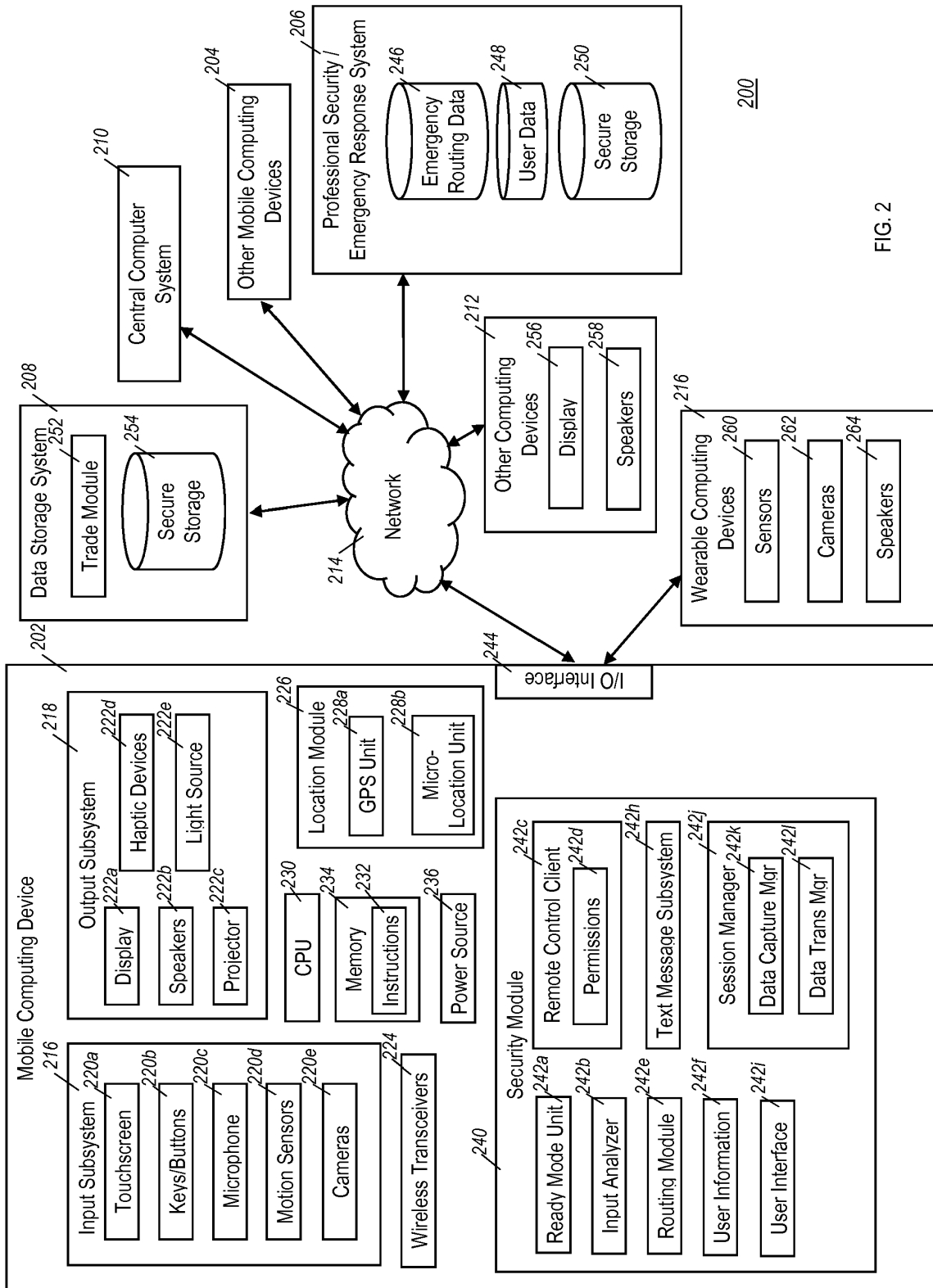


FIG. 2

300

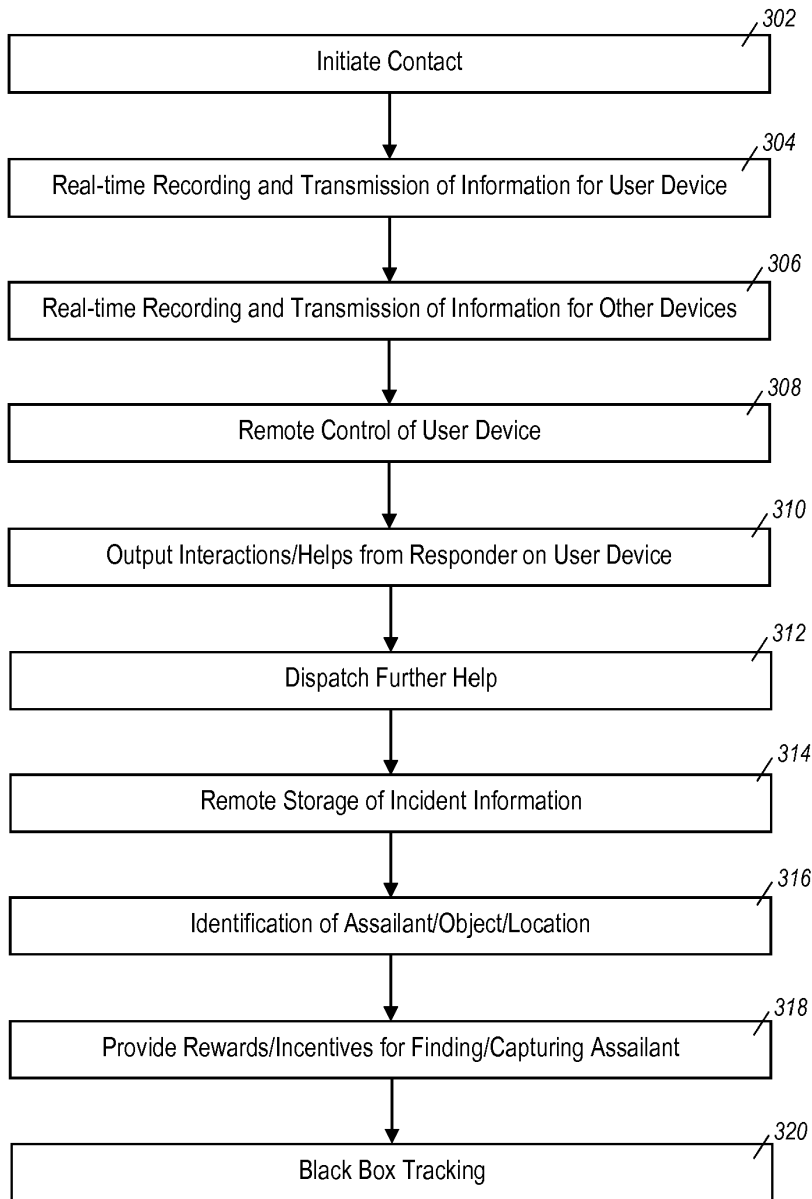


FIG. 3

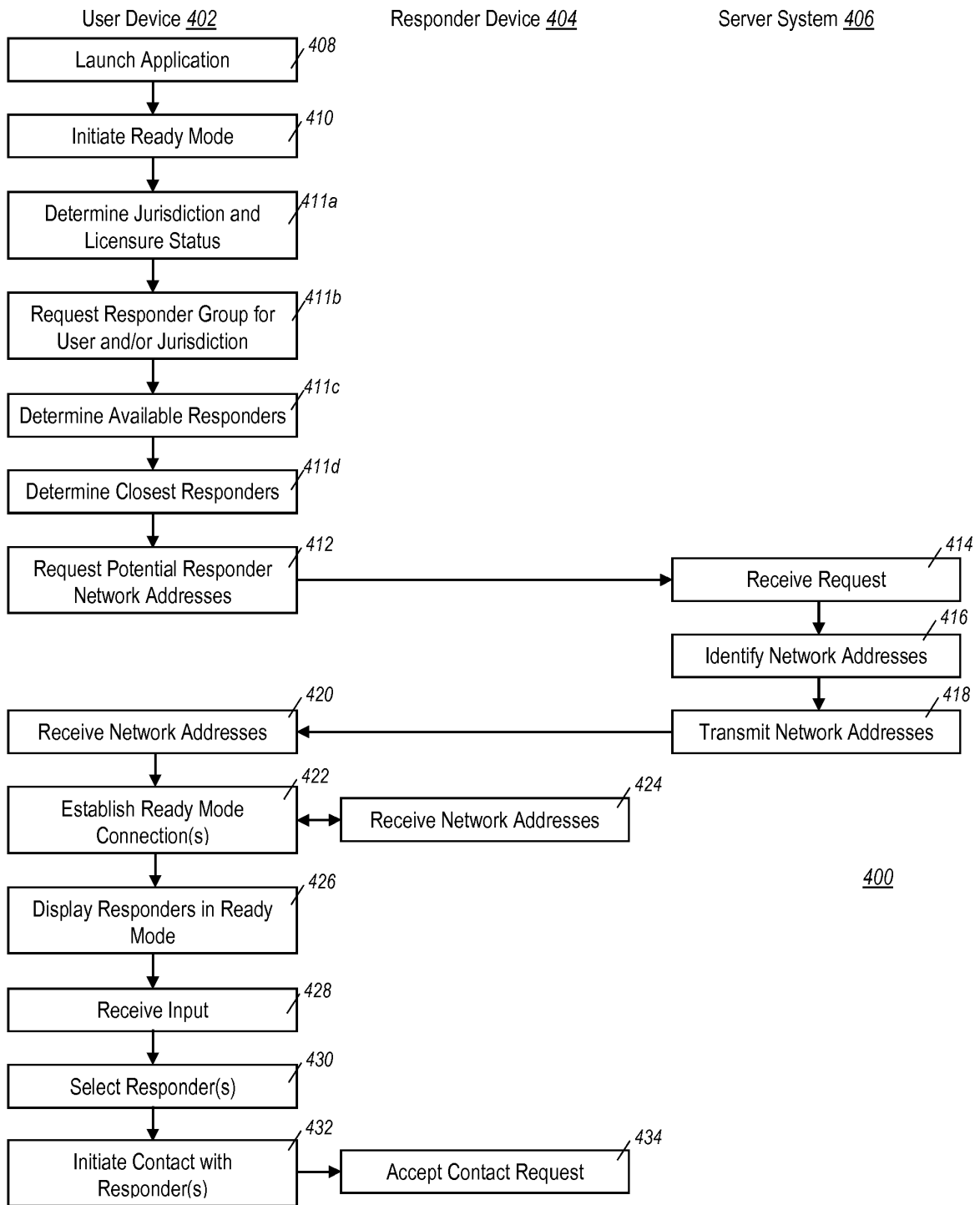


FIG. 4

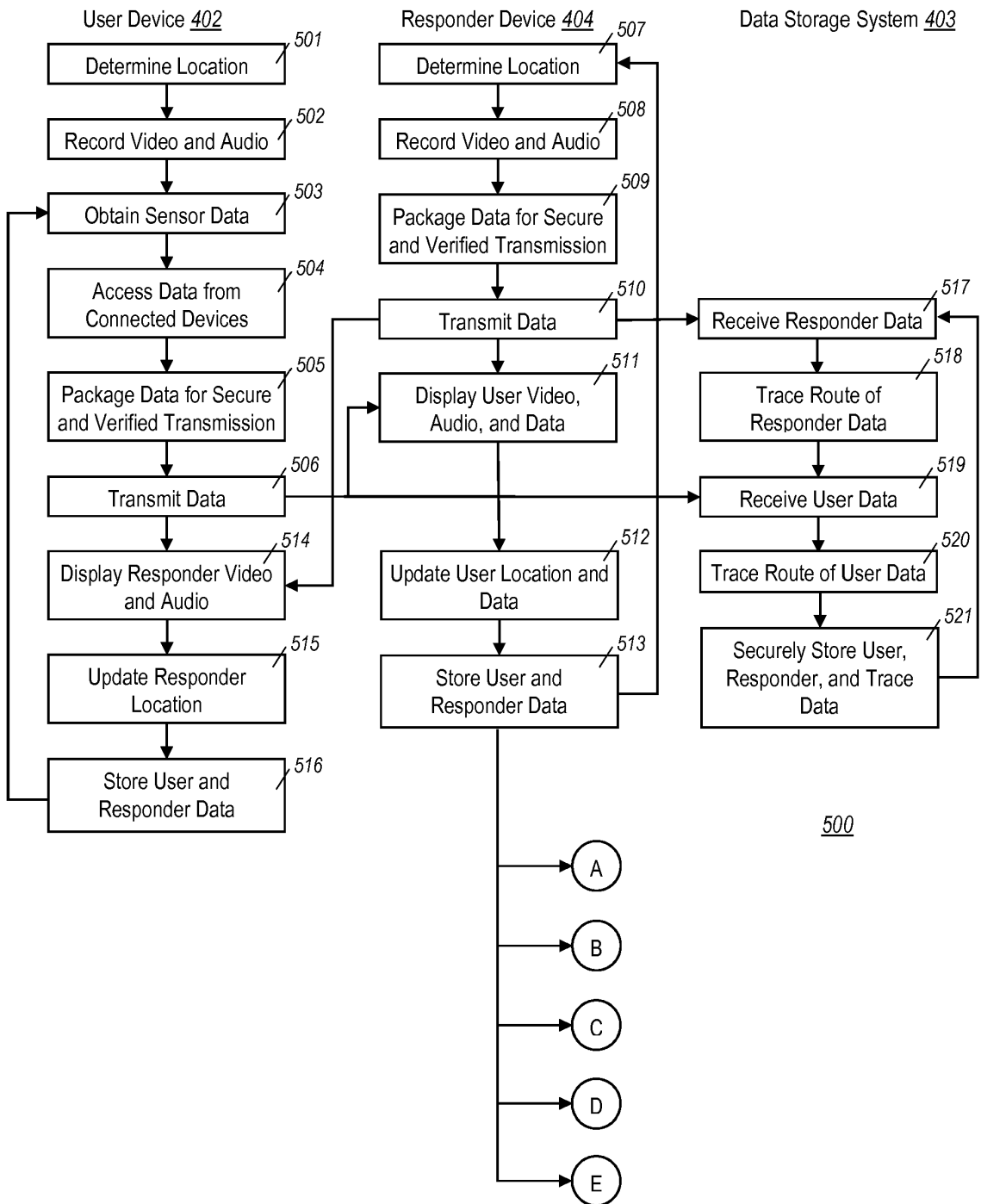
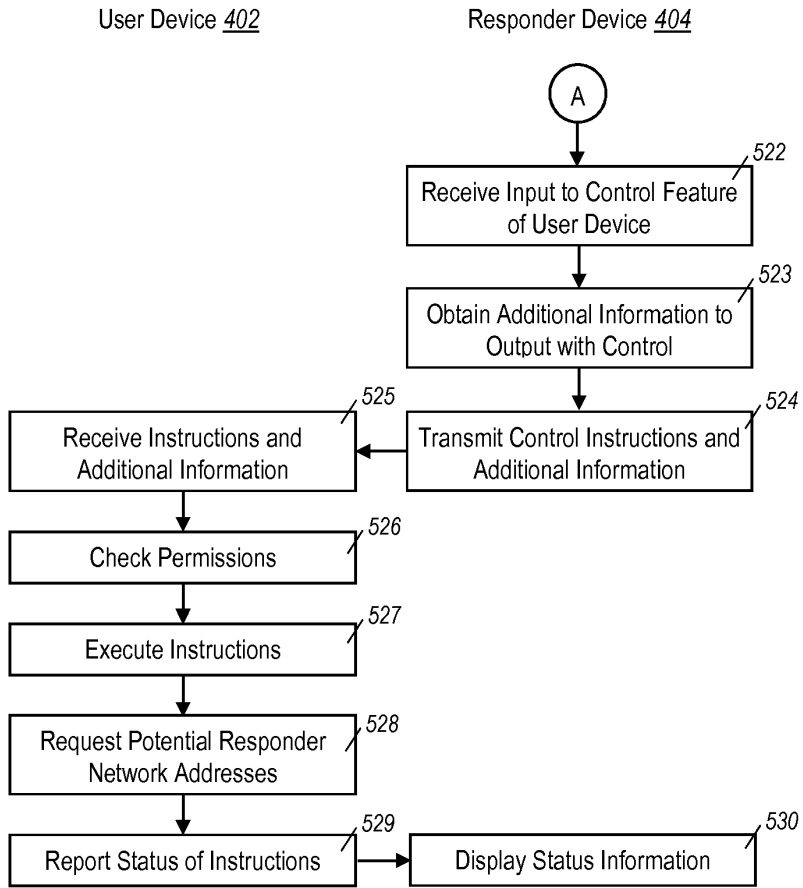
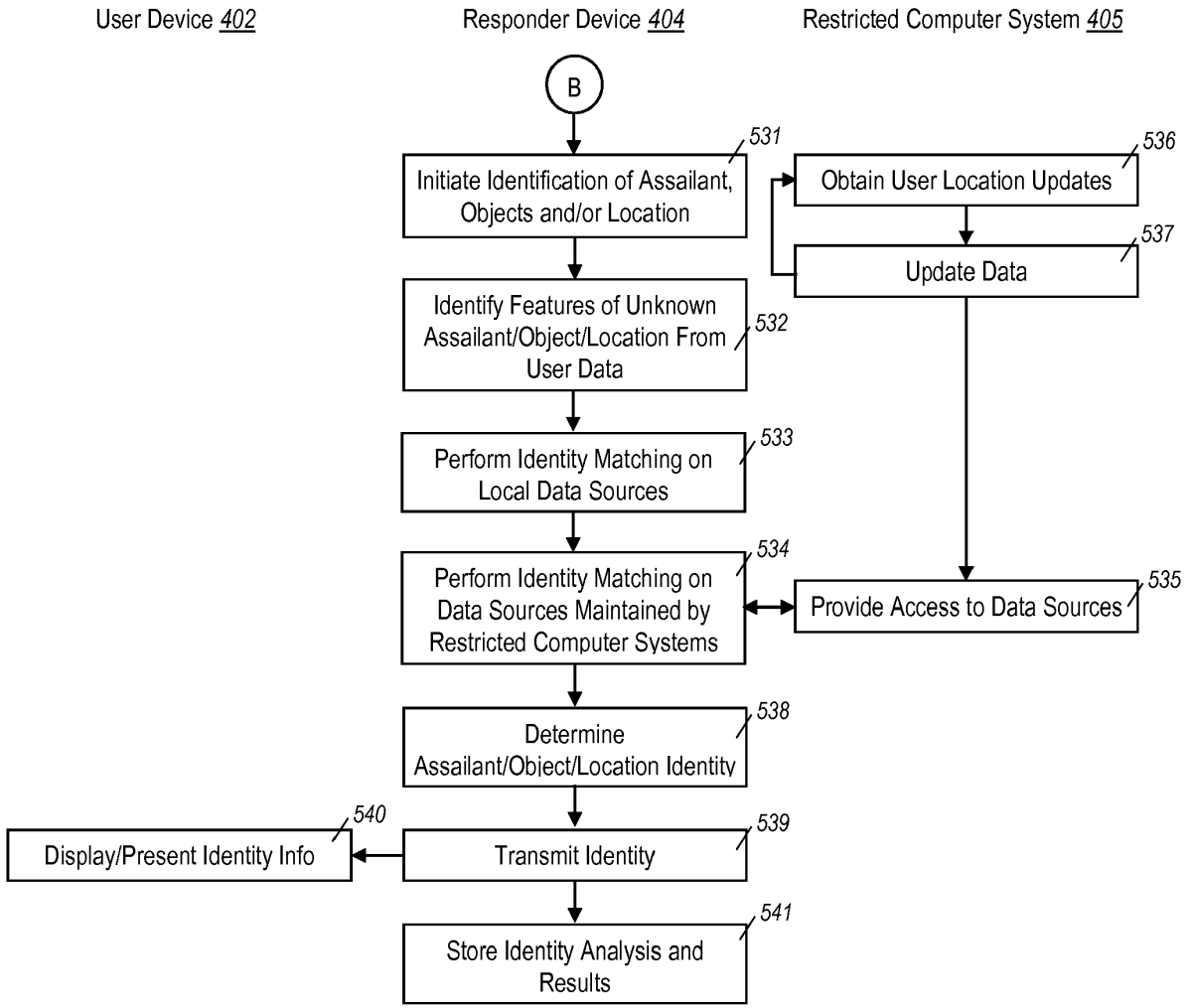


FIG. 5A



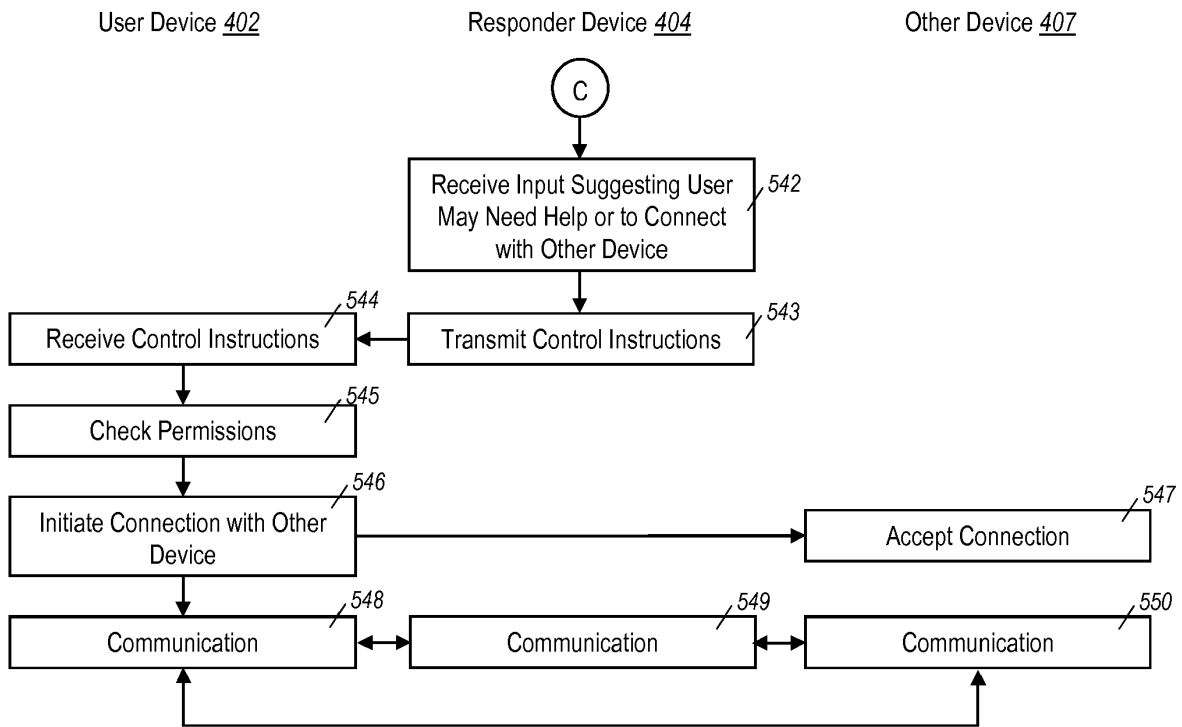
500

FIG. 5B



500

FIG. 5C



500

FIG. 5D

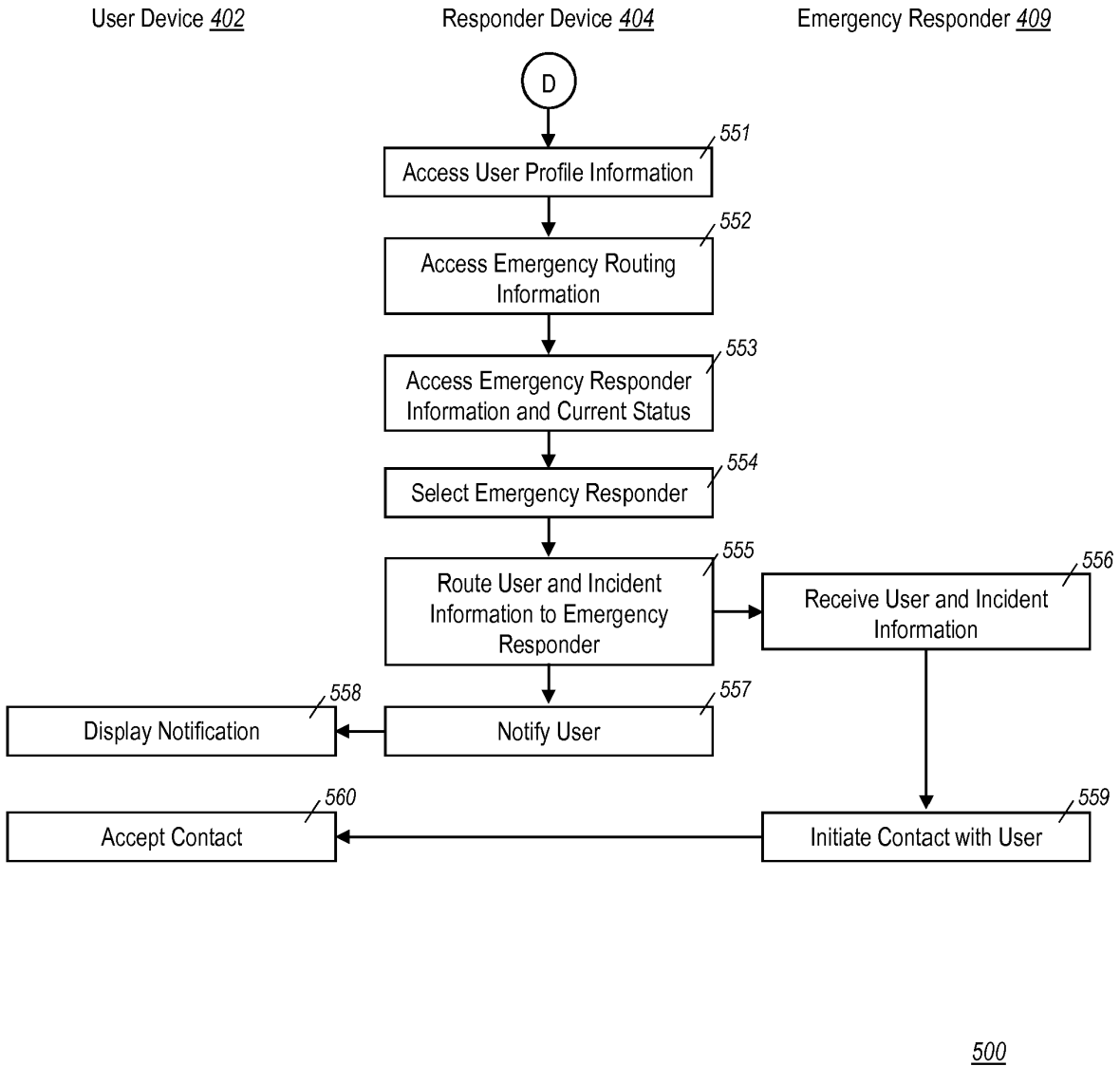
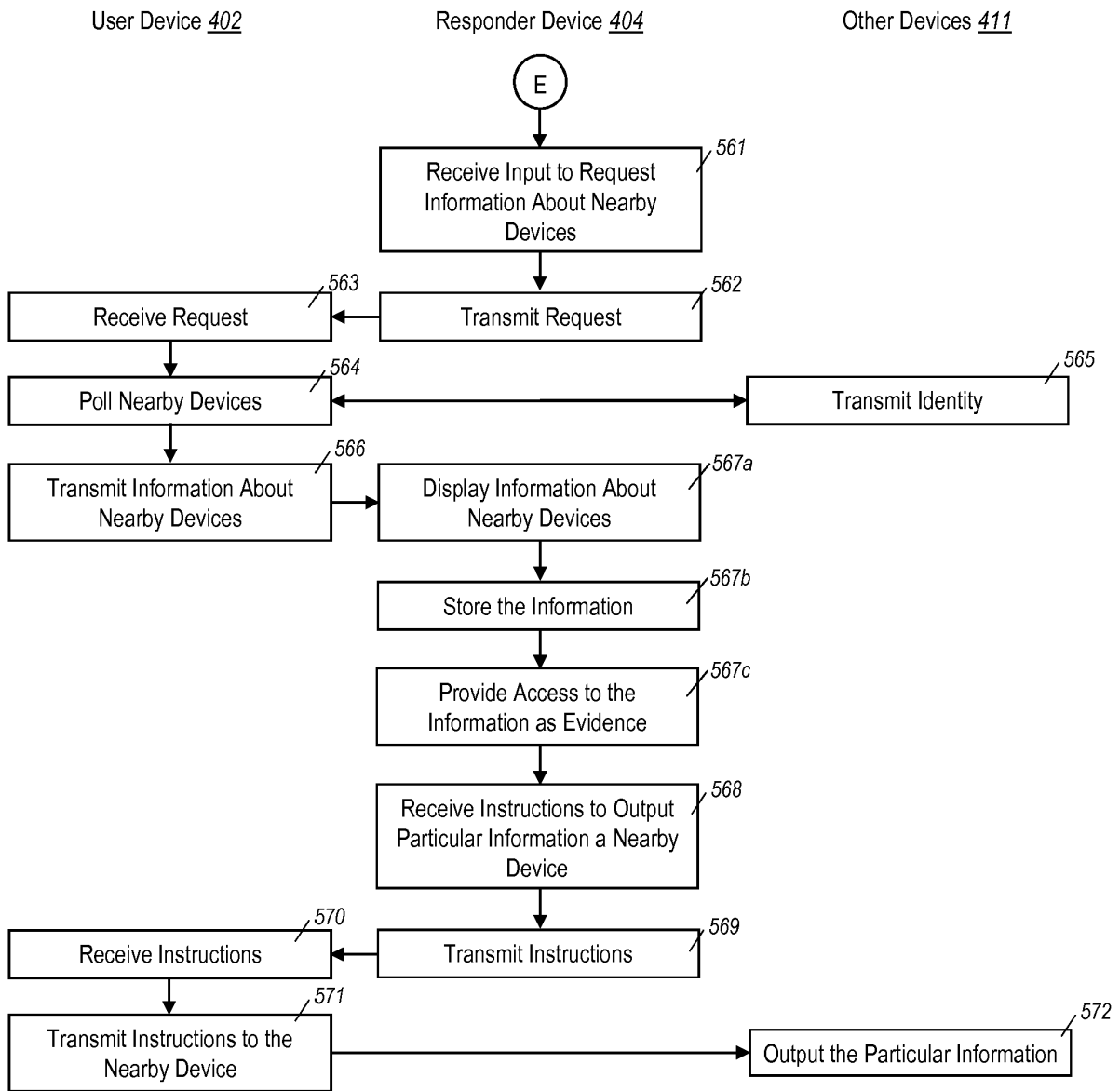


FIG. 5E



500

FIG. 5F



600

FIG. 6

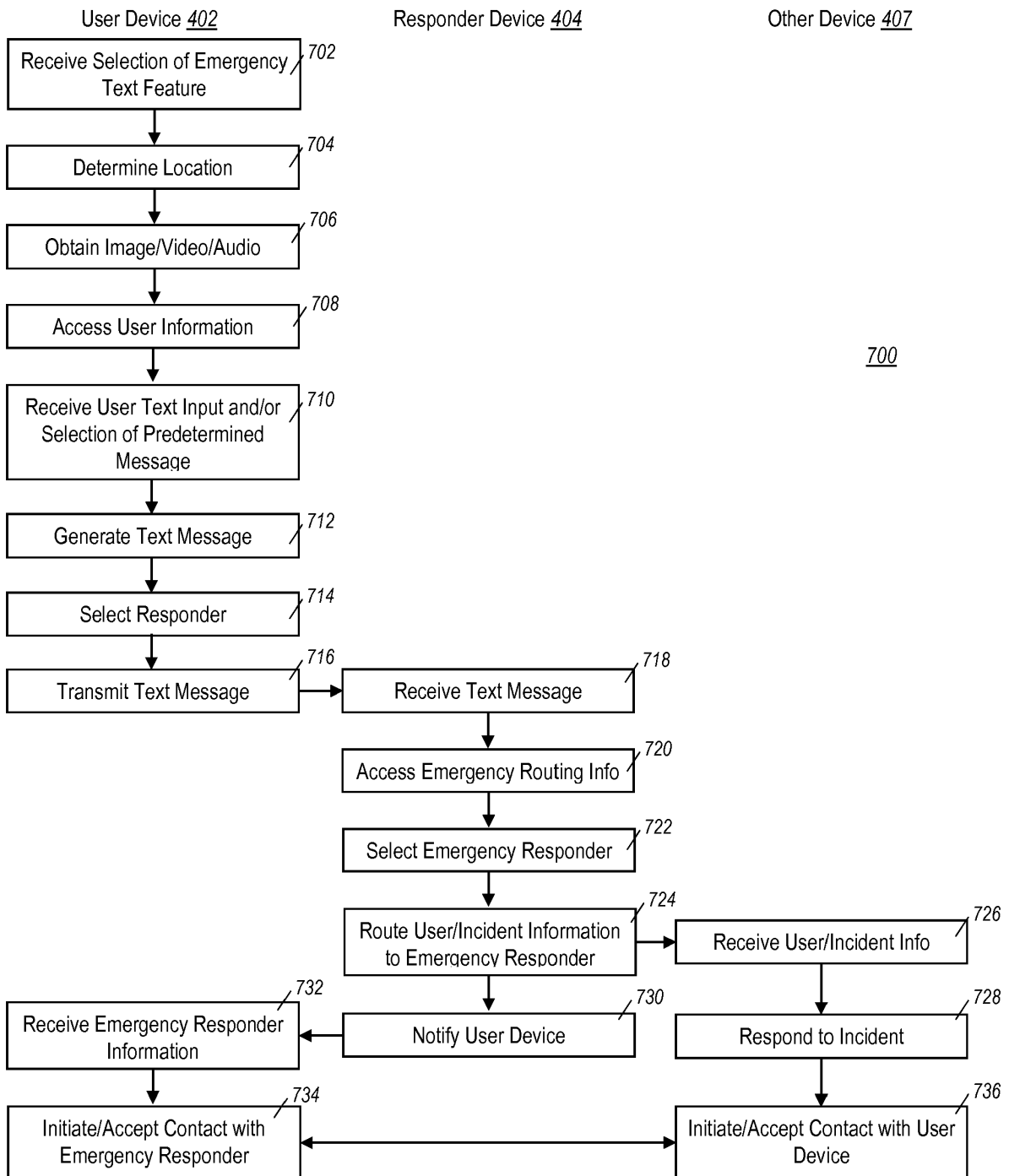
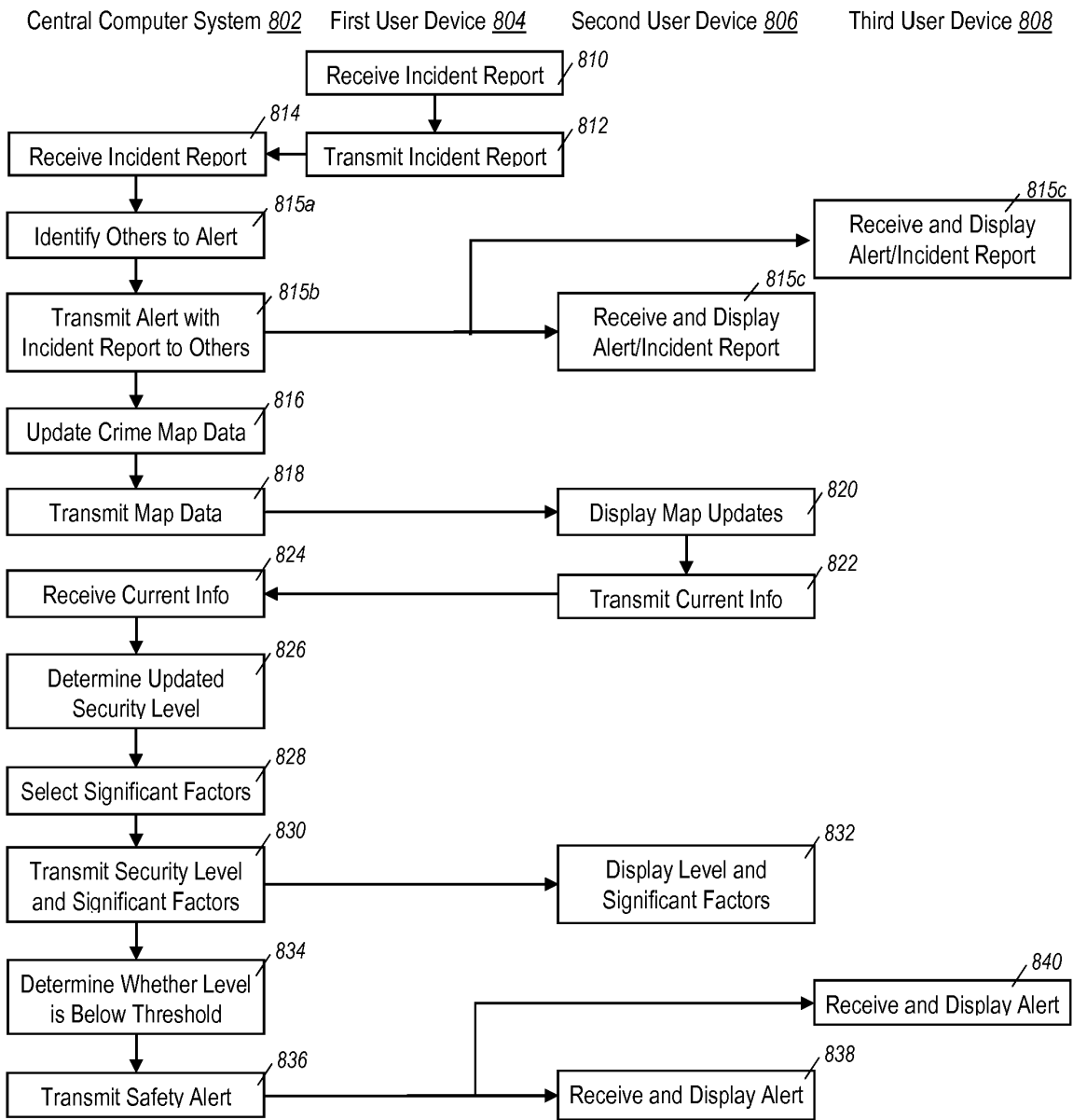
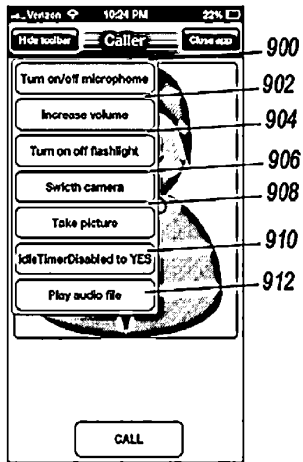


FIG. 7

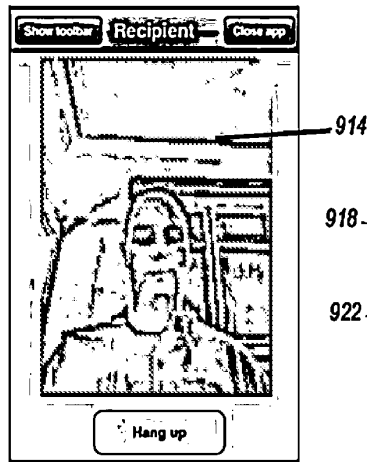


800

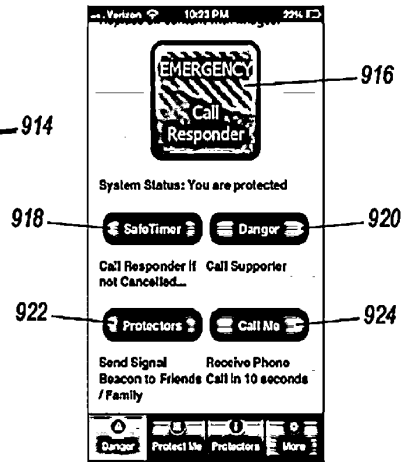
FIG. 8



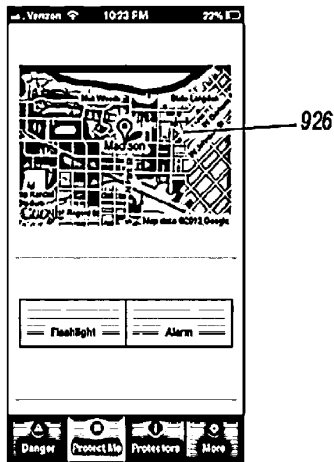
(A)



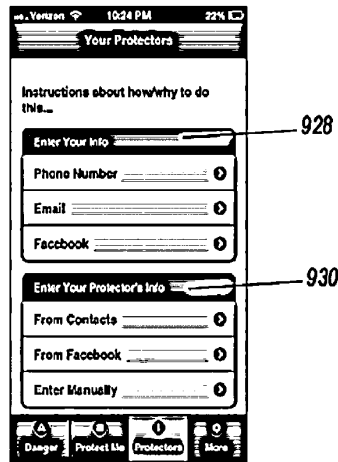
(B)



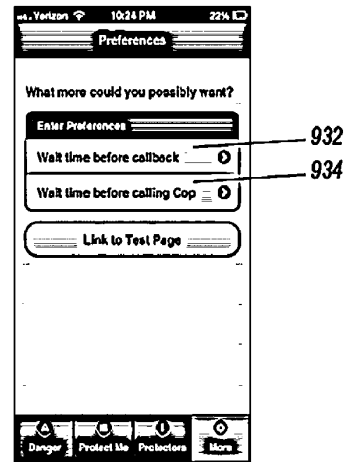
(C)



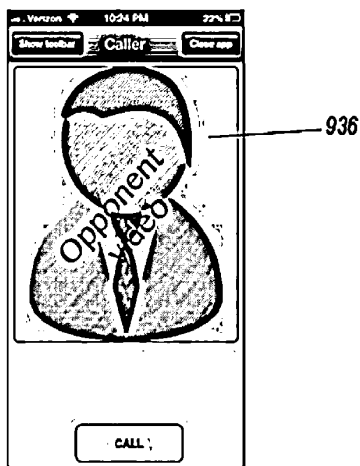
(D)



(E)



(F)



(F)

FIG. 9

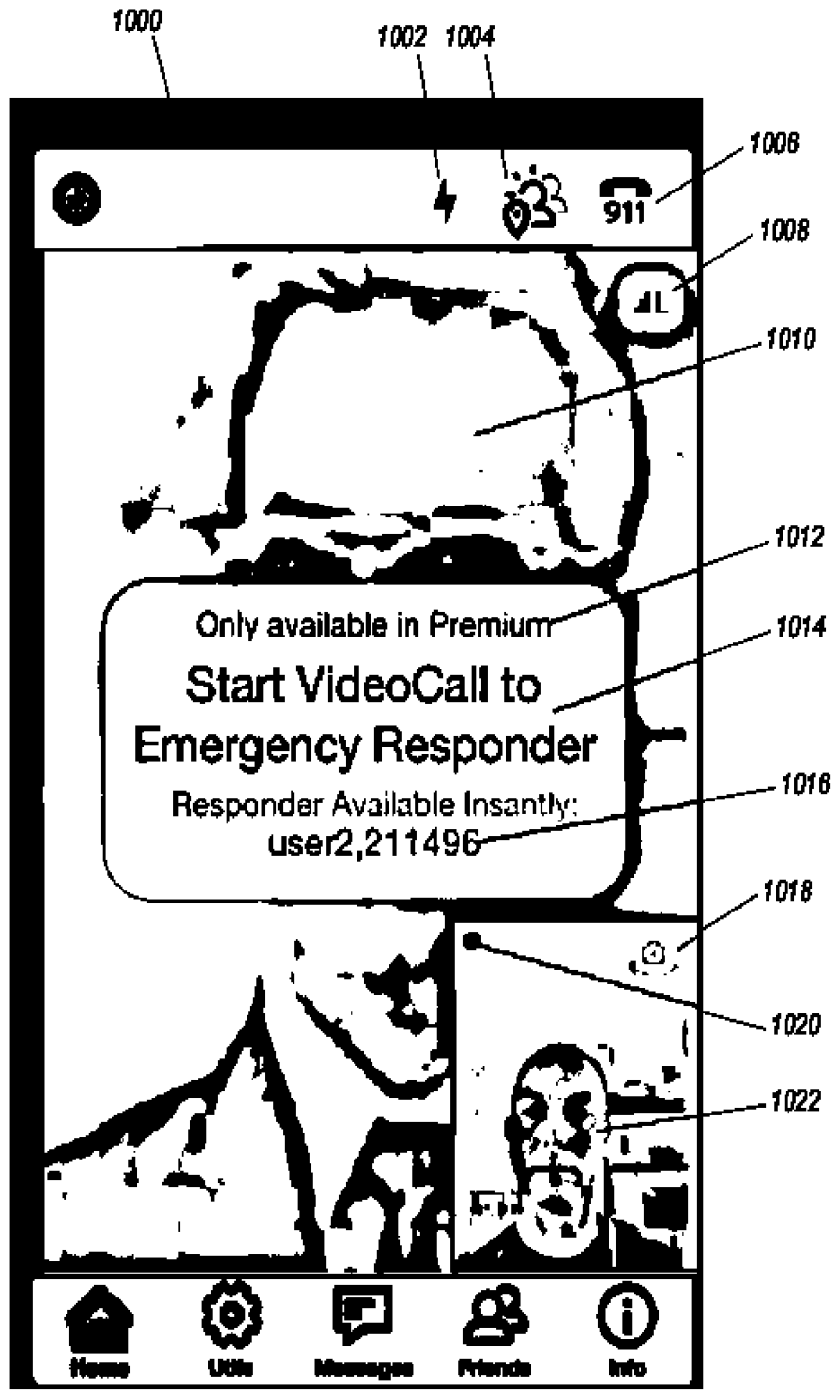


FIG. 10

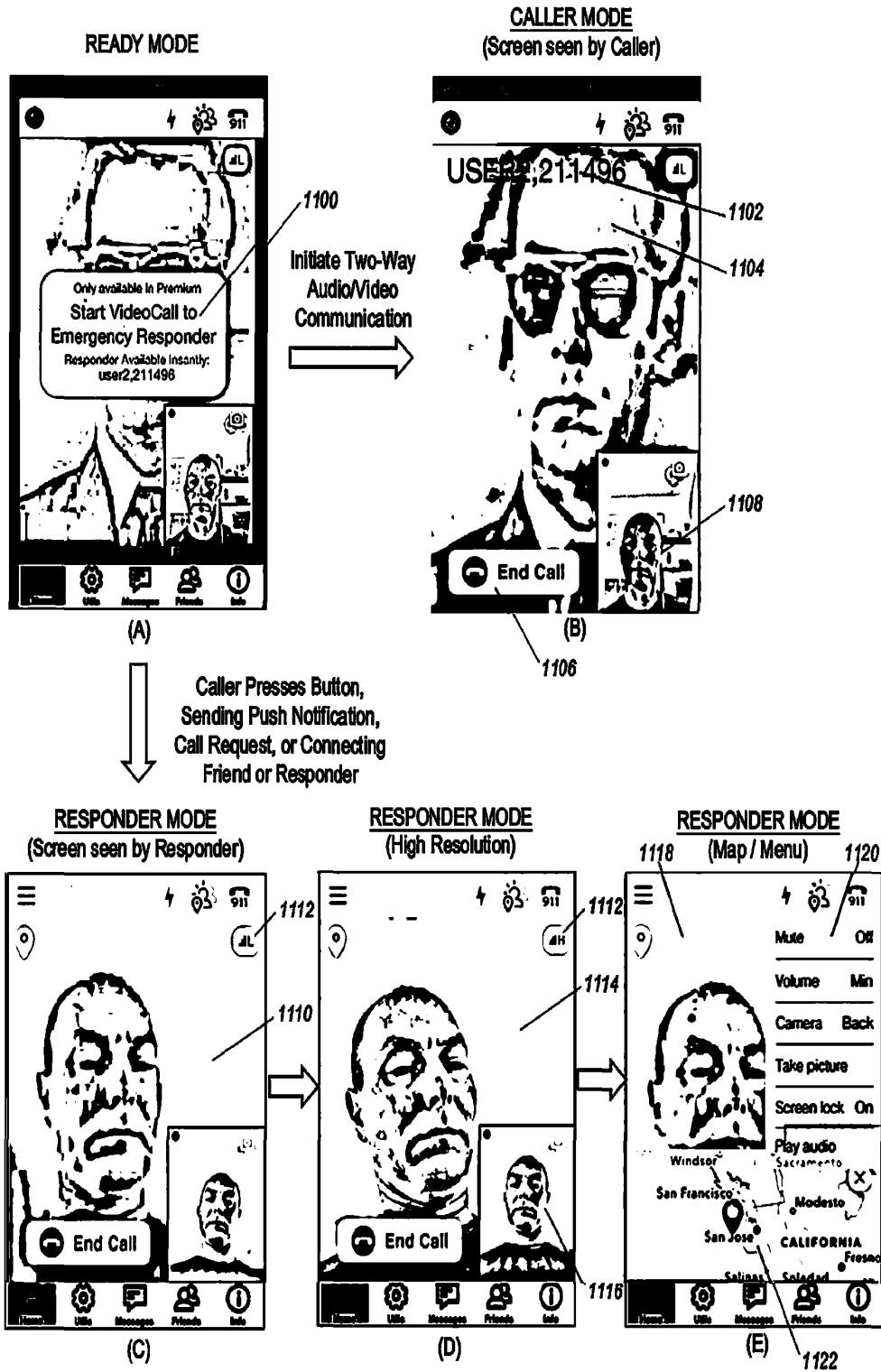
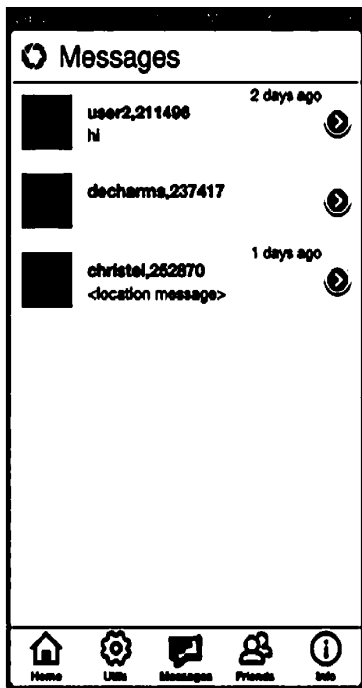
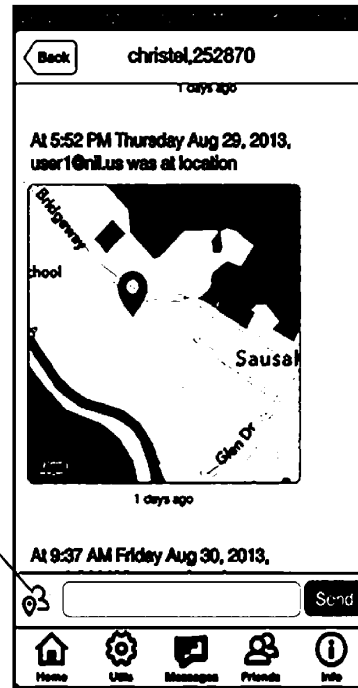


FIG. 11

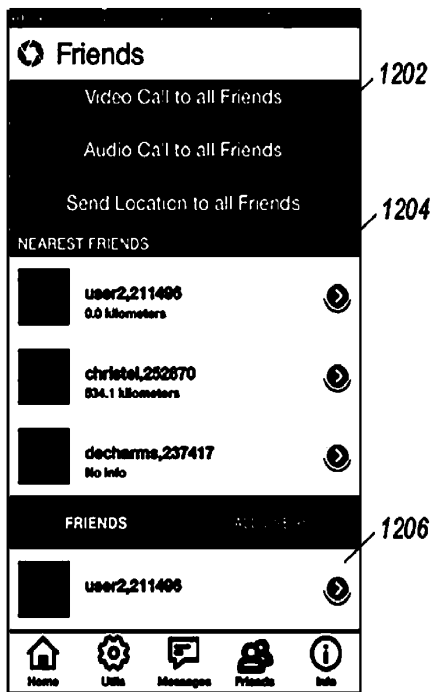


Initiate Two-Way
Instant
Messaging

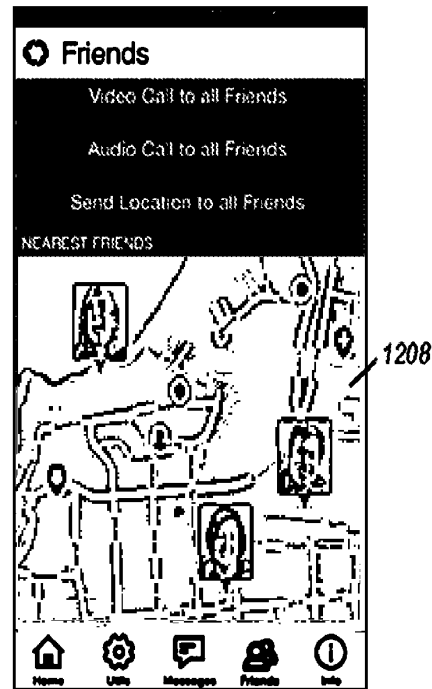


(A)

(B)



(C)



(D)

FIG. 12

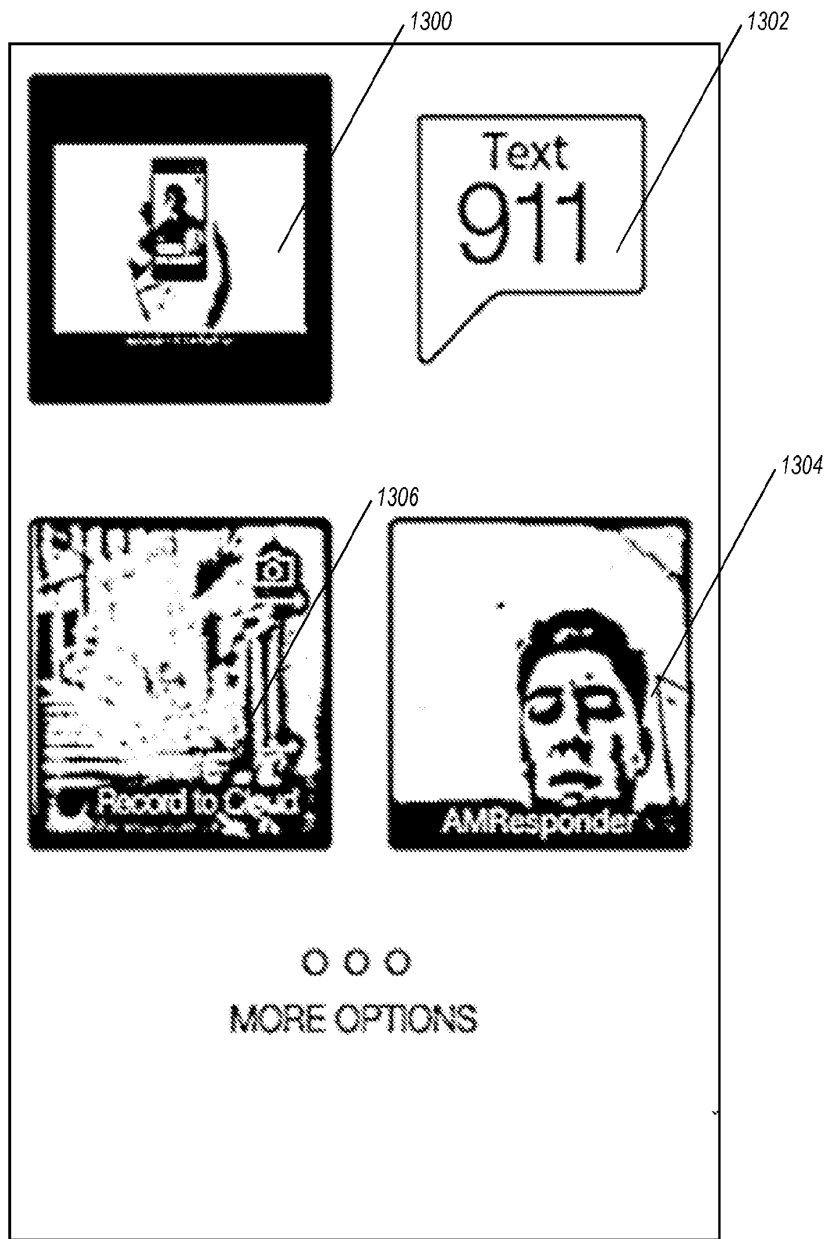


FIG. 13

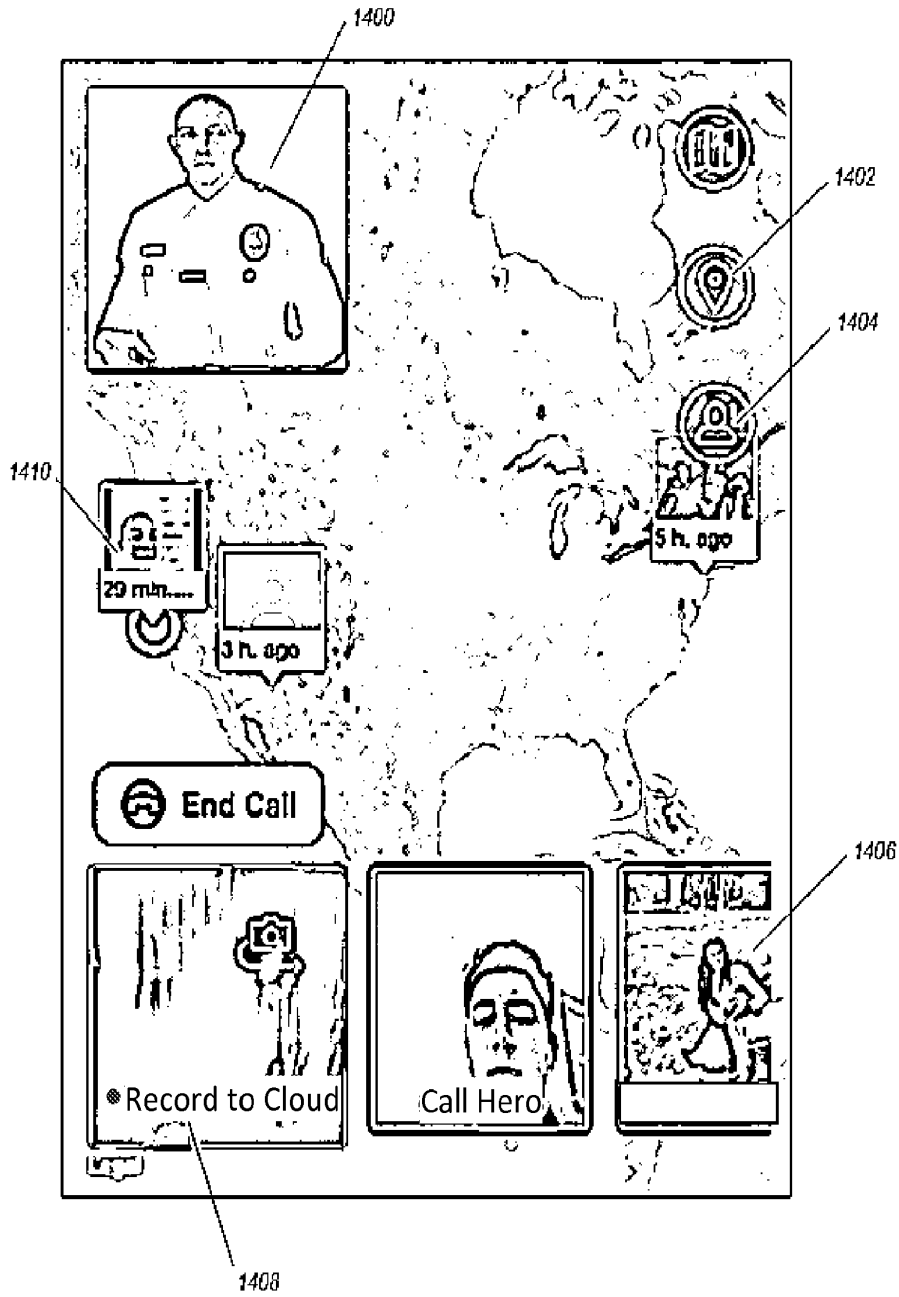


FIG. 14

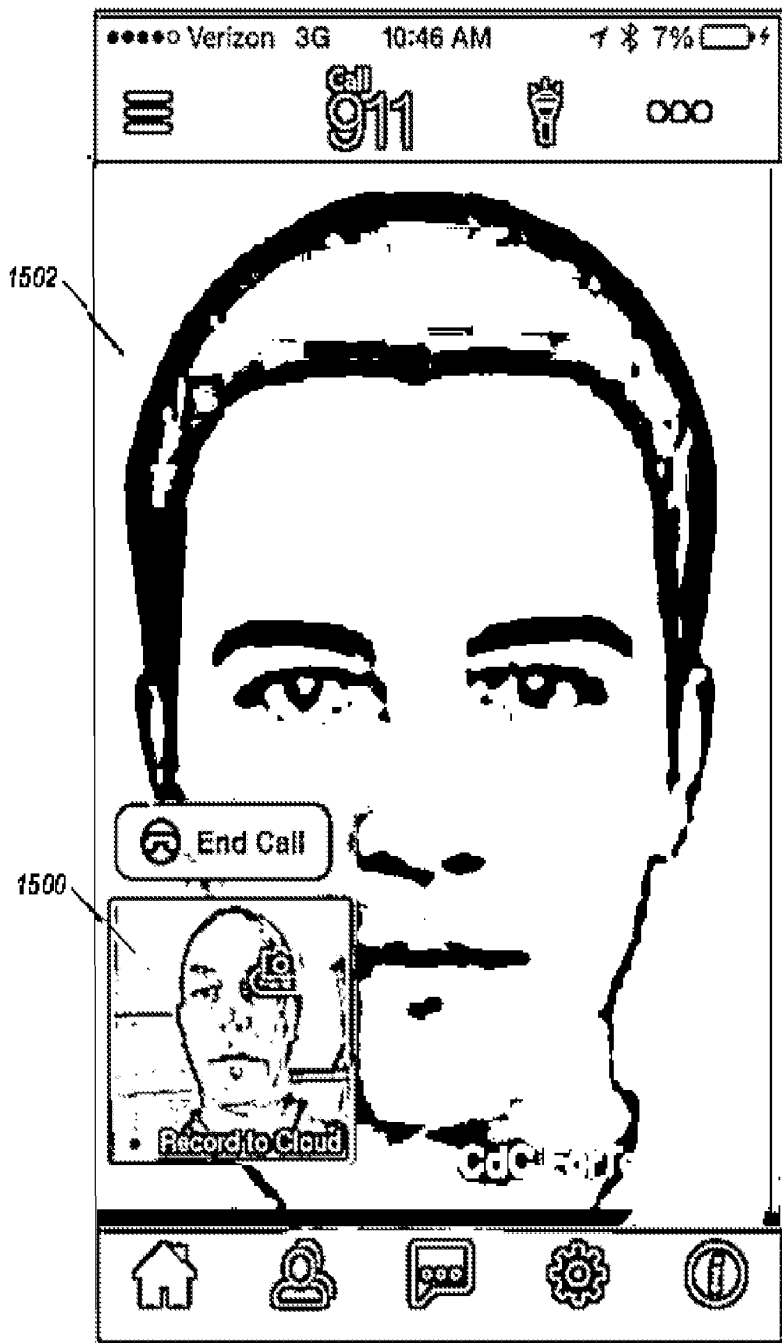


FIG. 15

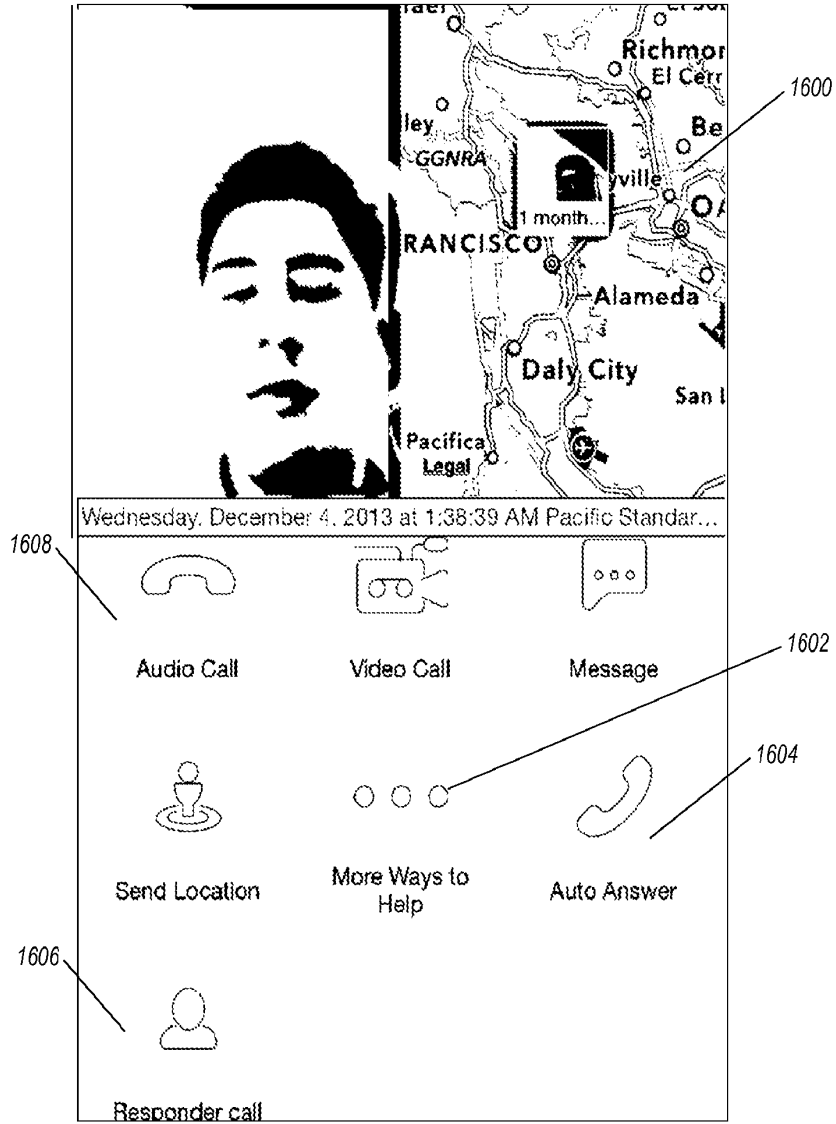


FIG. 16

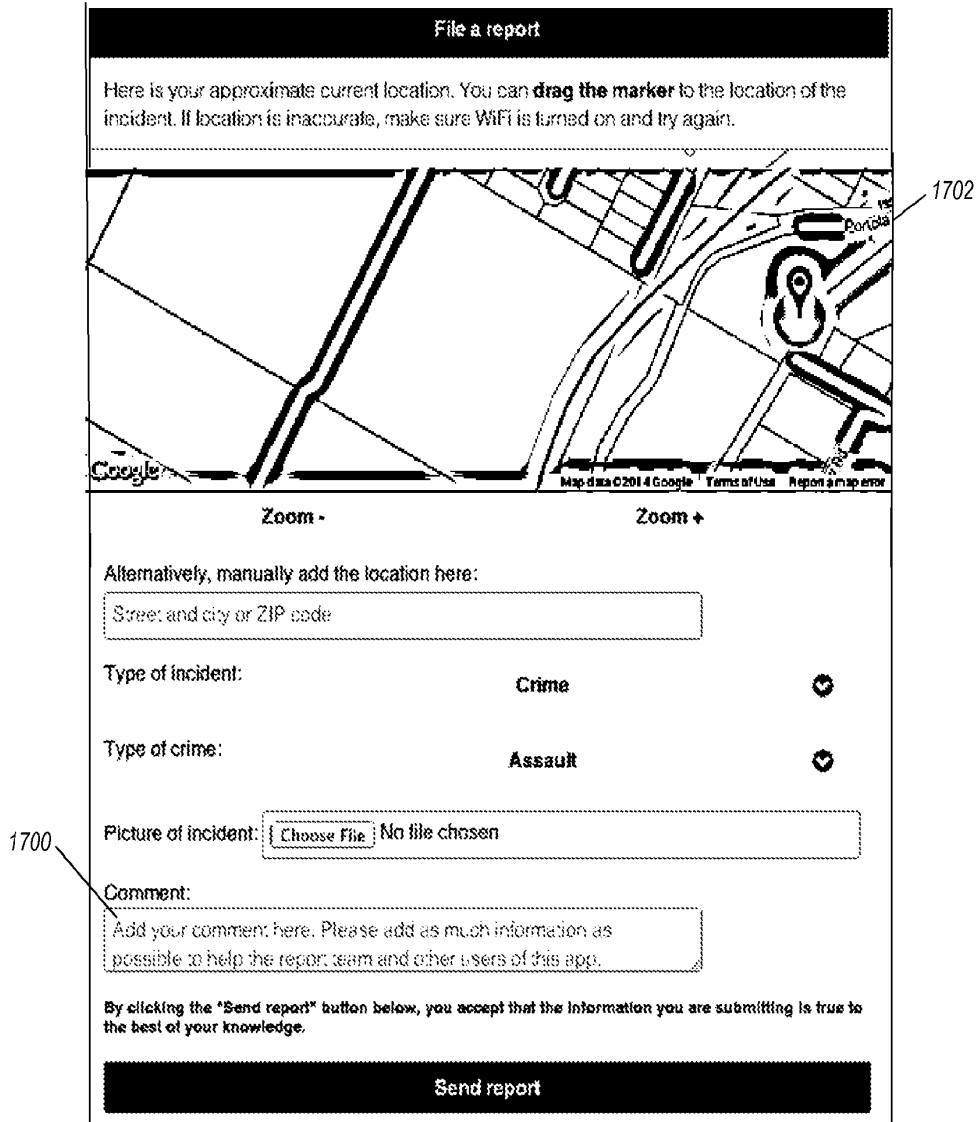


FIG. 17

The image shows a 'Settings' application screen with a black header. The form is organized into several sections separated by horizontal lines:

- Profile:** A 'Picture' field with a 'NO FILE CHOSEN' button and a dropdown arrow.
- Personal Information:** Fields for 'Age' (45), 'Height' (6 feet 2 inches), 'Weight' (Select weight...), 'Hair color' (Select hair color...), and 'Eye color' (Select...).
- Other Name(s):** A text input field with the placeholder 'Add your other name(s) here.'
- Language and Location:** Fields for 'First Language', 'Second Language', and 'Country', each with a 'Select...' dropdown.
- Addresses:** Three sections for 'Home address (tap to edit)', 'Work address (tap to edit)', and 'Billing address (tap to edit)'. Each section has a 'Safe word' field with the placeholder 'Add one word here, this will be your safe word'.
- Health:** Three sections: 'Allergies', 'Health conditions (if any)', and 'Health information', each with a text input field and a dropdown arrow.
- Automobile:** A section titled 'Automobile' with the instruction 'Ignore this section if you don't have a car.' It includes fields for 'Auto make' (Select an auto make...), 'Auto model' (Add the model of your auto here), 'Auto year' (Select year...), and 'Auto color' (Select a color...).
- Security Questions:** A section titled 'Security Questions' with the instruction 'These are used to prove your identity if you lose access to your account.' It includes a 'Security question 1' field (Select a question...) and an 'Answer 1' field.

FIG. 18A

Security Questions

These are used to prove your identity if you lose access to your account.

Security question 1: Select a question...

Answer 1:

Security question 2: Select a question...

Answer 2:

Security question 3: Select a question...

Answer 3:

Emergency contacts

Emergency contact 1 (tap to edit)

Emergency contact 2 (tap to edit)

Save

FIG. 18B

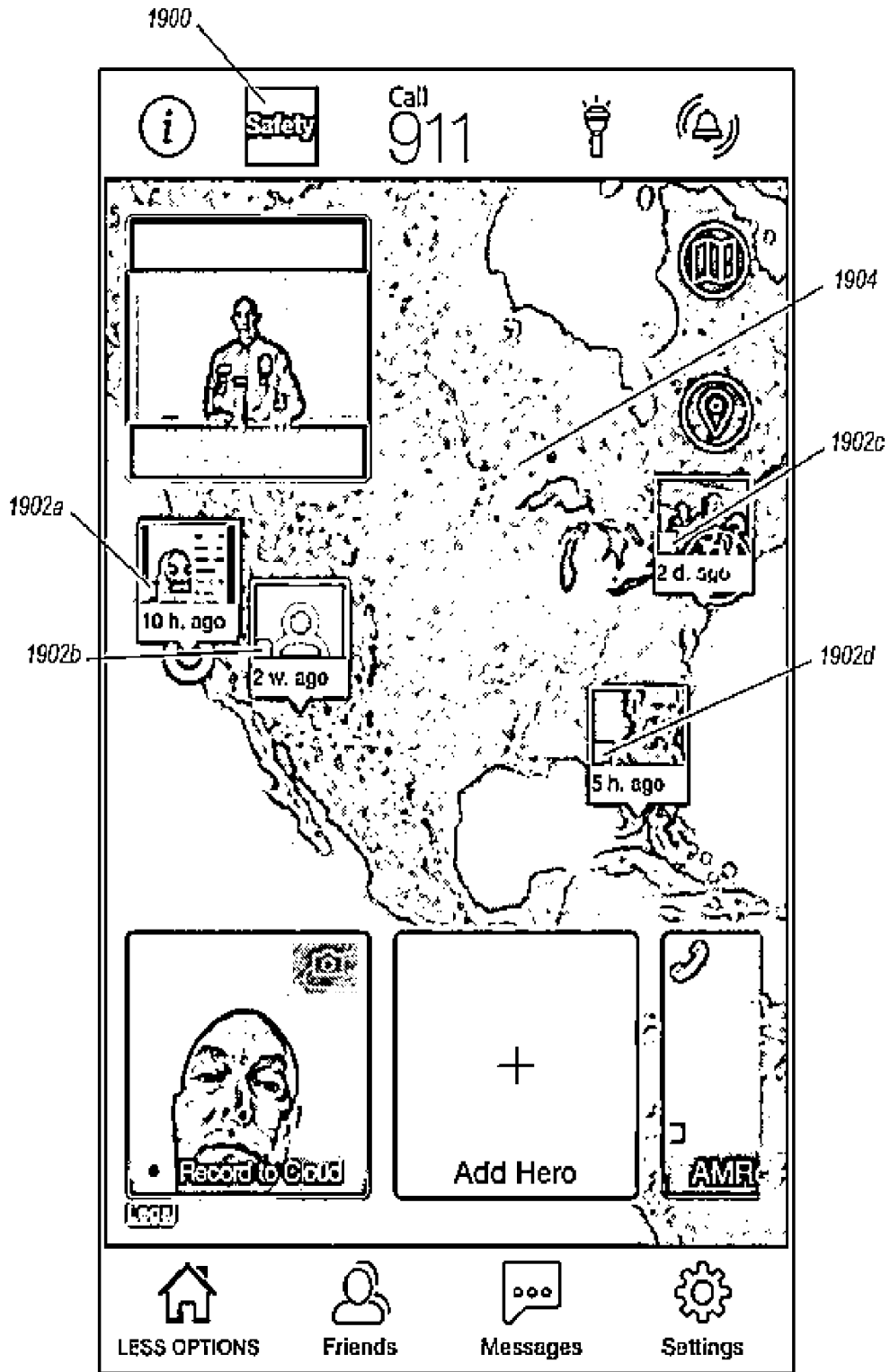


FIG. 19

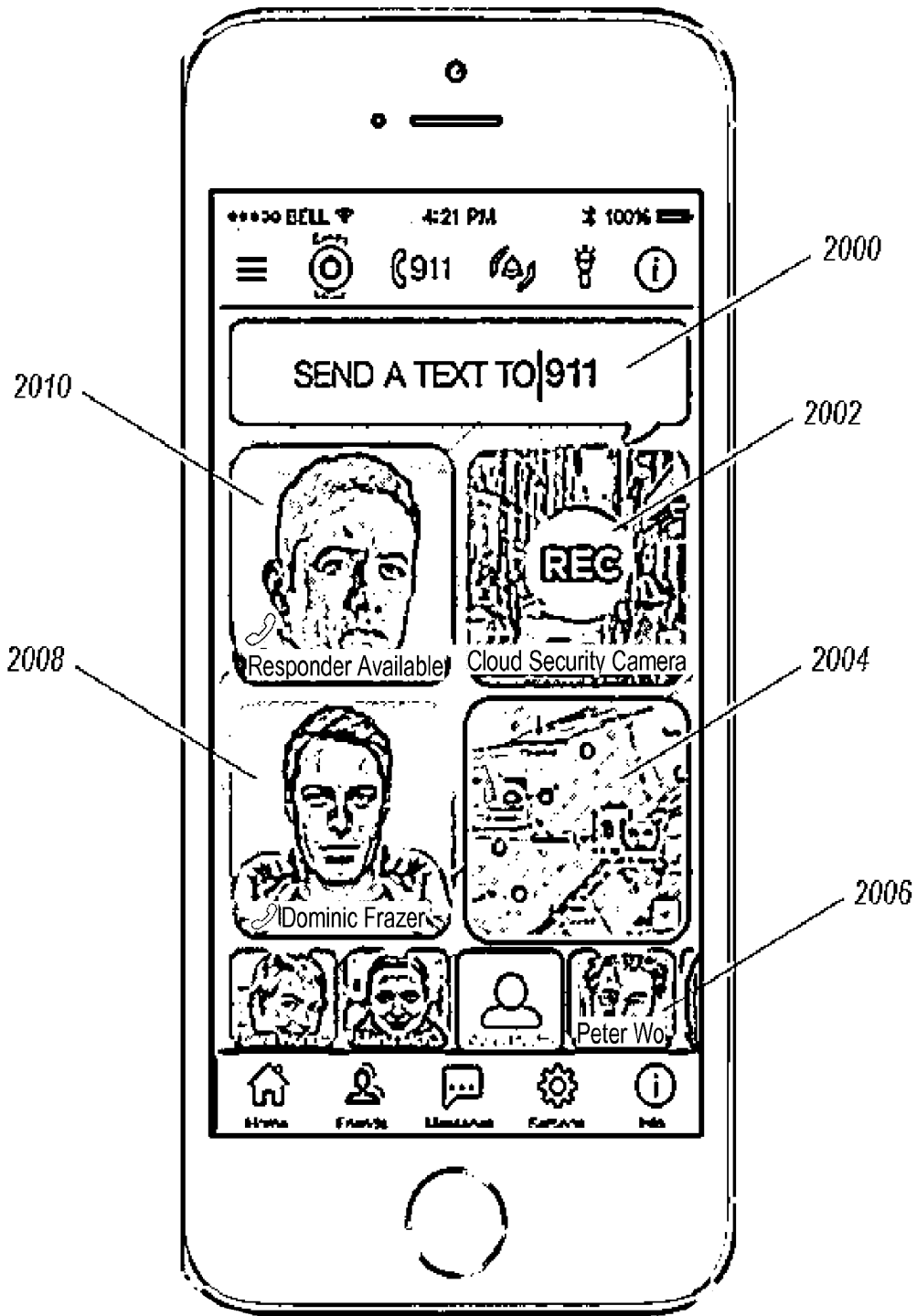


FIG. 20

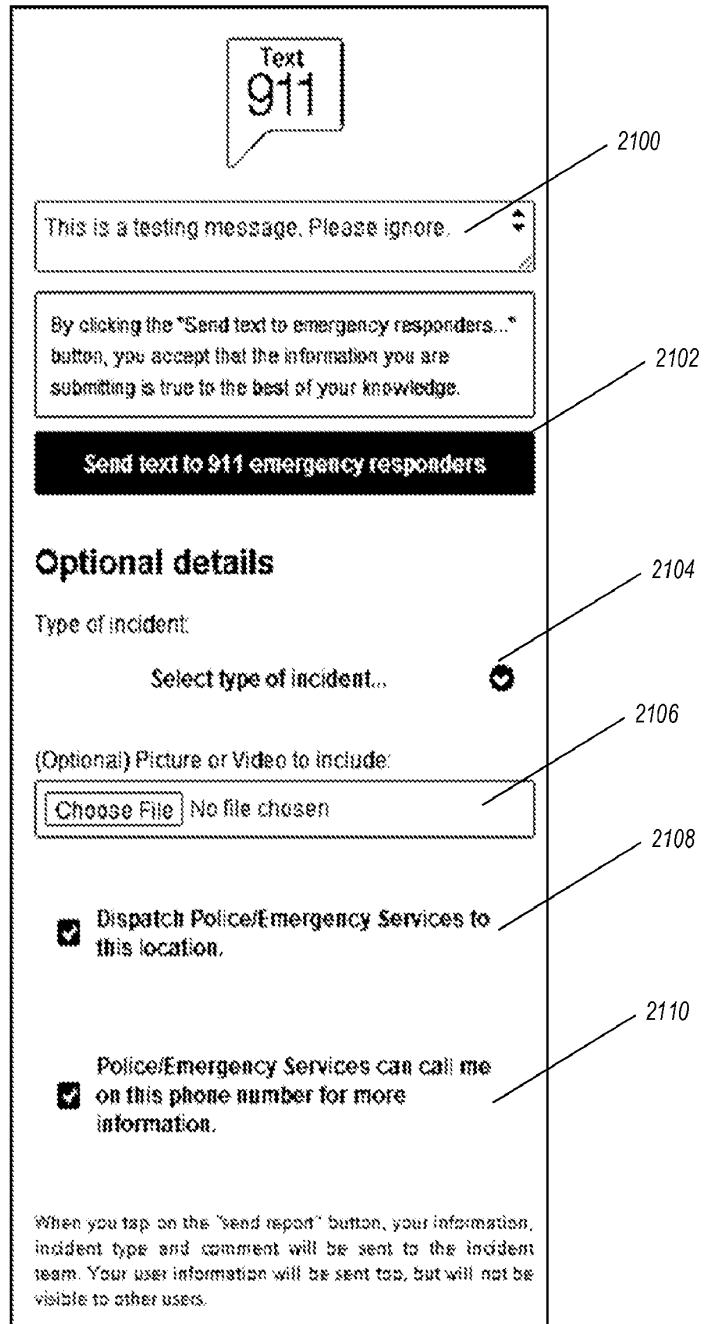


FIG. 21

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 17/943,956	Filed: September 13, 2022
Applicant: Carbyne Ltd.	Examiner: Lafontant, Gary
Inventor(s): Alexander Dizengof	Art Unit: 2646
Title: System, Method, and Computer-Readable Medium for Streaming Real-Time Data from a User Device	Confirmation No.: 2316

INFORMATION DISCLOSURE STATEMENT

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

Dear Examiner Lafontant:

Applicant requests that the documents identified on the Form PTO/SB/08a enclosed herewith be considered by the Examiner and made of record in this file. The Examiner is also asked to initial copies of the enclosed Form PTO/SB/08a to evidence such consideration.

The filing of this Information Disclosure Statement is not to be construed as an admission that the information cited in the statement is, or is considered to be, material to the patentability of the invention claimed in the above-identified application, or that it qualifies as prior art against any or all of the current claims. Further, no representation is made that a search has been performed.

This Information Disclosure Statement is being filed following the mailing of a first Office Action on the merits but prior to the mailing date of any of: (a) a final action under § 1.113; (b) a notice of allowance under § 1.311; or (c) an action that otherwise closes prosecution in the application. In accordance with 37 C.F.R. §1.97(c), Applicant respectfully requests that the \$104.00 fee due in connection with this Information Disclosure Statement be charged to Account No. 02-4467. Moreover, the Commissioner for Patents is hereby authorized to charge any additional fees necessitated by the filing of this paper, or credit any overpayment, to Account No. 02-4467.

Respectfully submitted,

BRYAN CAVE LEIGHTON PAISNER LLP
Two North Central Avenue
Suite 2100
Phoenix, AZ 85004-4406

/Cory G. Smith/
Cory G. Smith
Attorney for Applicant
Reg. No. 63,218
Tel. (602) 364-7442



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
Row 1: 17/943,956, 09/13/2022, Alexander Dizengof, 3010043.2, 2316
Row 2: 46019, 7590, 01/18/2023, BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX), TWO NORTH CENTRAL AVENUE, SUITE 2100, PHOENIX, AZ 85004
Row 3: EXAMINER LAFONTANT, GARY
Row 4: ART UNIT 2646, PAPER NUMBER
Row 5: NOTIFICATION DATE 01/18/2023, DELIVERY MODE ELECTRONIC

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

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

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

PXBCIPDocketing@bcplaw.com

<i>Applicant-Initiated Interview Summary</i>	Application No. 17/943,956	Applicant(s) Dizengof, Alexander		
	Examiner GARY LAFONTANT	Art Unit 2646	AIA (First Inventor to File) Status Yes	Page 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	Title	Type
GARY LAFONTANT	Primary Examiner	Video Conference
Cory Smith	Attorney	
George Chen	Attorney	
Alex Dizengof	Attorney	

Date of Interview: 12 January 2023

Issues Discussed:

35 U.S.C. 103

The above representatives argues that Piett does not teach the independent claim 1 because the application does not teach any separate APP to launch a video conference but only the embedded user mobile phone browser associated with WebRTC feature can launch a video streaming by having a user click on a web link received in the user phone. The video streaming and the voice call are simultaneously in communication with the called public safety agency station. Examiner said that he will review the OA by taking into account of the above arguments. No agreement was reached in term of allowance.

/GARY LAFONTANT/ Examiner, Art Unit 2646	
<p>Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04</p> <p>Please further see: MPEP 713.04 Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b) 37 CFR § 1.2 Business to be transacted in writing</p>	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20170034353		2017-02-02	Bell et al.	
	2	20160037126		2016-02-04	Polyakov et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2014158562	WO		2014-10-02	Echostar Technologies LLC		

If you wish to add additional Foreign Patent Document citation information please click the Add button. Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	LAND MOBILE, Wireless Communications for Business, www.landmobile.com, October 2016.	
	2	TV News Central, "New App to Allow 999 Callers to Live Stream from the Scene of Emergencies," dated 22 October 2014, (downloaded 14 November 2022).	
	3	Directors Club NEWS, "Capita and West Midlands Fire Service Launch 999EYE," dated 7 November 2016, (downloaded 14 November 2022).	
	4	British APCO Conference, https://www.mobilemark.com/bapco-annual-conference-exhibition/, (downloaded 17 November 2022).	
	5	PageOne Website, https://www.pageone.co.uk/999eye-wins-bapco-innovation-award/, (downloaded 14 November 2022).	
	6	YouTube Video, "Two Years of 999eye," https://www.youtube.com/watch?v=8E-DVij0km8, dated 15 November 2018, (viewed 21 November 2022).	

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	<input type="text"/>	Date Considered	<input type="text"/>
--------------------	----------------------	-----------------	----------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Cory Smith/	Date (YYYY-MM-DD)	2023-01-06
Name/Print	Cory Smith	Registration Number	63218

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour 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. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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.



(43) International Publication Date
2 October 2014 (02.10.2014)

(51) International Patent Classification:

H04N 21/2343 (2011.01) H04N 21/422 (2011.01)
H04N 21/266 (2011.01) H04N 21/658 (2011.01)
H04N 21/41 (2011.01) H04N 21/845 (2011.01)

(21) International Application Number:

PCT/US2014/018263

(22) International Filing Date:

25 February 2014 (25.02.2014)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/779,979 13 March 2013 (13.03.2013) US
13/900,357 22 May 2013 (22.05.2013) US

(71) Applicant: ECHOSTAR TECHNOLOGIES L.L.C.
[US/US]; 100 Inverness Terrace East, Englewood, Colorado 80112 (US).

(72) Inventor: KUMMER, David, A.; 8947 Green Meadows Lane, Highlands Ranch, Colorado 80126 (US).

(74) Agents: BAUNACH, Jeremiah, J. et al.; Seed Intellectual Property Law Group PLLC, Suite 5400, 701 Fifth Avenue, Seattle, Washington 98104-7064 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,

BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

Published:

- with international search report (Art. 21(3))

(54) Title: SYSTEMS AND METHODS FOR SECURELY PROVIDING ADAPTIVE BIT RATE STREAMING MEDIA CONTENT ON-DEMAND

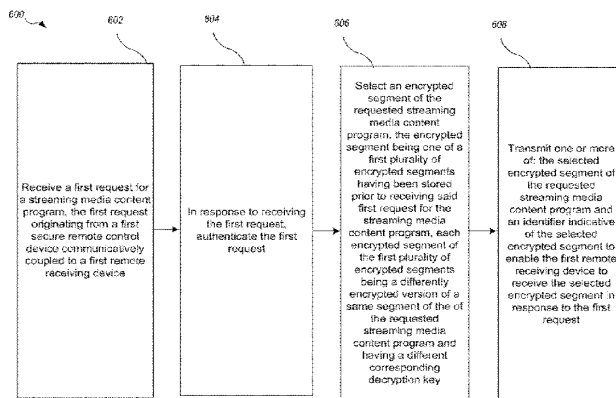


Fig. 6

(57) Abstract: A system for securely providing adaptive bit rate streaming media content on-demand may include a security server of a program distributor that selects, based on a received authorized request, which of a differently encrypted stored versions of a "special segment" of the requested program to deliver to the receiving device during the transmission of the requested program. The selection may be based on a pseudo-random selection process per request for the program based on an identifier of the request associated with the remote control device. The selection of which of the differently encrypted stored versions of the "special segment" of the ordered program to deliver may be based on the current session. The secure remote then sends to the receiving device the correct decryption key for the receiving device to decrypt the particular encrypted version selected of the "special segment" to be sent to the receiving device.

WO 2014/158562 A1

SYSTEMS AND METHODS FOR SECURELY PROVIDING ADAPTIVE BIT RATE STREAMING MEDIA CONTENT ON-DEMAND

TECHNICAL FIELD

The technical field relates to delivering media content, and particularly to providing media content securely to multiple different recipients.

BRIEF SUMMARY

Each of multiple receiving devices at various customer locations may request the same or different streaming media content (e.g., stored at a content storage system of a content delivery network) on-demand using video on-demand (VOD) or other available on-demand services and/or applications associated with, in communication with or running on the respective receiving devices. Differently encrypted versions of particular, i.e., "special" segments of the ordered program may already be stored at the content storage system of the content delivery network. Each differently encrypted version of a special segment has a different decryption key which is for decrypting the corresponding differently encrypted version of that special segment. In contrast, other segments, i.e., "non-special" segments of the requested program, are each encrypted once using the same or different encryption key from each other.

In conjunction with this request for the streaming media program, the secure remote sends a unique code associated with the secure remote to the content storage system of the content delivery network via the receiving device. If the request is approved and/or authenticated by the program distributor and/or the content storage system of the content delivery network based on the unique code, a security server of the program distributor may then send an authorization to the secure remote. For example, this may be an authorization code that allows or enables the secure remote to derive the decryption key for the "non-special" segments. The content storage system of

the content delivery network may then begin to transmit the stored encrypted program in response to the order. The secure remote then sends this decryption key, or a portion thereof, to the receiving device for decryption of those “non-special” segments.

During transmission of the requested program, or prior to the transmission, once the content storage system of the content delivery network encounters one of those “special segments” that have been differently encrypted a number of times and stored on the content storage system of the content delivery network, the content storage system of the content delivery network may send a request to the program distributor for information regarding which of the differently encrypted stored versions of the “special segment” of the ordered program to deliver to the receiving device during the transmission of the ordered program to the receiving device.

The program distributor may then select, or have pre-selected based on the received authorized request, which of the differently encrypted stored versions of the “special segment” of the ordered program to deliver to the receiving device during the transmission of the ordered program based on a random or pseudo-random selection process. This may also be based on the particular request or order for the streaming media content program, such as by performing the random or pseudo-random selection process per request for the program based on an identifier of the request associated with the remote control device. In this manner, the selection of which of the differently encrypted stored versions of the “special segment” of the ordered program to deliver is based on the current session, i.e., current request and associated transmission, for the requested program.

The secure remote then sends to the receiving device the correct decryption key for the receiving device to decrypt the particular encrypted version selected of the “special segment” to be sent to the receiving device. The secure remote may have pre-stored corresponding encryption and/or decryption keys and/or corresponding encryption algorithms and information

associating which of these correspond with each of the differently encrypted versions of the “special” segment(s).

BRIEF DESCRIPTION OF THE DRAWINGS

The components in the drawings are not necessarily to scale relative to each other. Like reference numerals designate corresponding parts throughout the several views.

Figure 1 is an overview block diagram illustrating an example content distribution environment in which embodiments of securely providing adaptive bit rate streaming media content on-demand may be implemented, according to one example embodiment.

Figure 2 is a block diagram illustrating elements of an example receiving device used in securely providing adaptive bit rate streaming media content on-demand, according to one example embodiment.

Figure 3 is a block diagram of an example content storage system of a content delivery network in operable communication with multiple remote example receiving devices such as that of Figure 2 to which streaming media content is securely provided on-demand, according to one example embodiment.

Figure 4 is a block diagram illustrating components of an example embodiment of a secure remote-control device used in securely providing adaptive bit rate streaming media content on-demand in wireless communication with a receiving device and a presentation device, according to one example embodiment.

Figure 5 is a diagram illustrating an example of how particular segments of a streaming media content program may be differently encrypted a number of times and stored in a content storage system of a content delivery network in a system for securely providing adaptive bit rate streaming media content on-demand, according to one example embodiment.

Figure 6 is a flow diagram of a method in a security server in a media content transmission system shown in Figure 1 through Figure 4 of providing adaptive bit rate streaming media content on-demand, according to one example embodiment.

Figure 7 is a flow diagram of method in a secure remote control shown in figures 1, 3 and 4, of securely providing adaptive bit rate streaming media content on-demand, according to one example embodiment.

Figure 8 is a flow diagram of method in a content storage system of a content delivery network shown in Figure 1 through Figure 4, of securely providing adaptive bit rate streaming media content on-demand, according to one example embodiment.

DETAILED DESCRIPTION

Video on Demand (VOD) is a system which allows a user to select, watch and/or listen to video and audio content on demand. For example “Internet Television” and “Internet Protocol Television” (IPTV) are systems through which various media content is delivered using the Internet protocol (IP) suite over a packet-switched network such as the Internet, instead of being delivered through traditional channels using terrestrial, satellite signal, and cable television formats. In such situations, the device used to receive the content may often be other user equipment than the set-top box provided by the cable provider, satellite provider, or other program distributor to which the customer subscribes for such on-demand services. These may include various user devices such as a television, a digital video recorder (DVR), digital versatile disc (DVD) player, personal computer (PC), tablet device, game machine, smart phone, mobile device or other computing device or media player not provided by or controlled by the cable provider, satellite provider, or other program distributor to which the customer subscribes for the on-demand services. In such situations, it may be more difficult for the cable provider, satellite provider or program distributor to securely provide such on demand

services to those devices and also accommodate adaptive bit rate streaming, because of the decryption which must usually occur at the device receiving the content in order to present the content to the user and due to there being no unique hardware or software control of such devices by the service provider or program distributor.

Also, it may take significant processing power and time to encrypt the content differently per on-demand request and/or per user based on information received from a secure remote control device associated with the user to provide the additional security and control desired. However, the systems and methods described herein provide solutions which overcome this difficulty and enable the cable service provider, satellite service provider or other program distributor to more easily provide streaming media content to such devices in a secure manner, while also accommodating adaptive bit rate streaming, using a secure remote control device of the user that may be provided or configured by the cable service provider, satellite service provider or other program distributor.

Figure 1 is an overview block diagram illustrating an example content distribution environment in which embodiments of securely providing adaptive bit rate streaming media content on-demand may be implemented, according to one example embodiment.

Before providing additional details regarding the operation and constitution of methods and systems for securely providing adaptive bit rate streaming media content on-demand, the example content distribution environment 102, within which such a system may operate, will briefly be described.

In the content distribution environment 102, audio, video, and/or data service providers, such as television service providers, provide their customers a multitude of video and/or data programming (hereafter, collectively and/or exclusively "programming"). Such programming is often provided by use of a receiving device 118 communicatively coupled to a presentation device

120 configured to receive the programming. The programming may include any type of media content, including, but not limited to: television shows, news, movies, sporting events, advertisements, etc. In various embodiments any of this programming may be provided as a type of programming referred to as streaming media content, which is generally digital multimedia data that is substantially constantly received by and presented to an end-user or presented on a device while being delivered by a provider from a stored file source. Its verb form, "to stream", refers to the process of delivering media in this manner. The term refers to how the media is delivered rather than the media itself.

The receiving device 118 interconnects to one or more communications media or sources. For example, the various media content may be delivered as data using the Internet protocol (IP) suite over a packet-switched network such as the Internet or other packet-switched network. The underlying connection carrying such data may be via a cable head-end, satellite antenna, telephone company switch, cellular telephone system, Ethernet portal, off-air antenna, or the like. The receiving device 118 may receive a plurality of programming by way of the communications media or sources, or may only receive programming via a particular channel or source described in greater detail below. In some embodiments, based upon selection by a user, the receiving device 118 processes and communicates the selected programming to the presentation device 120. Also, in some embodiments, the presentation device 120 may also be a receiving device 118 or have a receiving device 118 integrated within it.

For convenience, examples of a receiving device 118 may include, but are not limited to devices such as, or any combination of: a "television converter," "receiver," "set-top box," "television receiving device," "television receiver," "television," "television recording device," "satellite set-top box," "satellite receiver," "cable set-top box," "cable receiver," "media player," "digital video recorder (DVR)," "digital versatile disk (DVD) Player," "computer," "mobile device," "tablet computer," "smart phone," "MP3 Player," "handheld

computer,” and/or “television tuner,” etc. Accordingly, the receiving device 118 may be any suitable converter device or electronic equipment that is operable to receive or playback programming. Further, the receiving device 118 may itself include user interface devices, such as buttons or switches. In some example embodiments, the receiving device 118 may be configured to receive and decrypt content according to various digital rights management (DRM) and other access control technologies and architectures as part of the process of securely providing adaptive bit rate streaming media content on-demand to the receiving device 118, which will be described in further detail below.

In many applications, a remote-control device (“remote”) 128 is operable to control the receiving device 118 and/or the presentation device 120. The remote 128 typically communicates with the receiving device 118 using a suitable wireless medium, such as infrared (“IR”), radio frequency (“RF”), or the like, including, but not limited to devices using Bluetooth® wireless technology, Wi-Fi® wireless technology, Radio Frequency for Consumer Electronics (RF4CE) wireless technology, etc. In the present example embodiment, the remote 128 is a “secure” remote configured according to an example embodiment to enable securely providing adaptive bit rate streaming media content on-demand to the receiving device 118, which will be described in further detail below. In other embodiments, the secure remote 128 could instead or also be a smart phone, tablet or other device that could have a secure software program and/or hardware elements that would allow the service provider to use it with better security resources than the receiving device 118.

Examples of a presentation device 120 may include, but are not limited to, one or a combination of the following: a television (“TV”), a personal computer (“PC”), a sound system receiver, a digital video recorder (“DVR”), a compact disk (“CD”) device, DVD Player, game system, tablet device, smart phone, mobile device or other computing device or media player, and the like. Presentation devices 120 employ a display, one or more speakers, and/or other

output devices to communicate video and/or audio content to a user. In many implementations, one or more presentation devices 120 reside in or near a customer's premises 116 and are communicatively coupled, directly or indirectly, to the receiving device 118. Further, the receiving device 118 and the presentation device 120 may be integrated into a single device. Such a single device may have the above-described functionality of the receiving device 118 and the presentation device 120, or may even have additional functionality.

A content provider 104 provides program content, such as television content, to a distributor, such as the program distributor 106. Example content providers include television stations which provide local or national television programming and special content providers which provide premium based programming, pay-per-view programming and on-demand programming.

Program content (*i.e.*, a program including or not including advertisements), is communicated to the program distributor 106 from the content provider 104 through suitable communication media, generally illustrated as communication system 108 for convenience. Communication system 108 may include many different types of communication media including those utilized by various different physical and logical channels of communication, now known or later developed. Non-limiting media and communication channel examples include one or more, or any operable combination of, telephone systems, the Internet, cable systems, fiber optic systems, microwave systems, asynchronous transfer mode ("ATM") systems, frame relay systems, digital subscriber line ("DSL") systems, radio frequency ("RF") systems, cellular systems, and satellite systems.

In at least one embodiment, the received program content is converted by the program distributor 106 into a suitable signal (a "program signal") that is ultimately communicated to the receiving device 118. Various embodiments of the receiving device 118 may instead receive programming

from program distributors 106 and/or directly from content providers 104 via locally broadcast RF signals, cable, fiber optic, Internet media, or the like via the communication system 108, such as from the content storage system of a content delivery network 122.

For example, Video on Demand (VOD) systems may allow a user of the receiving device 118 to select, watch and/or listen to video and audio content on demand. For example “Internet Television” and “Internet Protocol Television” (IPTV) are systems through which various media content is delivered using the Internet protocol (IP) suite over a packet-switched network such as the Internet represented by communication system 108 to the receiving device 118, instead of being delivered through traditional channels using terrestrial, satellite signal, and cable television formats of the communication system 108. In various example embodiments, such technologies are deployed within the content distribution environment 102 such as in subscriber-based telecommunications networks of the communication system 108 with high-speed access channels into the customer premises 116 via the receiving device 118 (e.g., a set-top box or other customer-premises equipment) to bring VOD services to the customer premises 116.

In various example embodiments, television VOD systems stream media content via the communications system 108 from files stored at the content storage system of the content delivery network 122, under direct or indirect control of the program distributor 106, to the receiving device 118. The content storage system of the content delivery network 122 may also comprise multiple separate storage facilities and streaming media content servers geographically separated from each other, each of which (also referred to as an “edge cache”) streams stored media content to particular customer locations based on a number of factors such as proximity of the customer premises 116 to the individual content storage system of the content delivery network 122 location or edge cache, load balancing parameters, current demand on the individual content storage system of the content delivery network 122, capacity

of the individual content storage system of the content delivery network 122, etc.

Television VOD systems may stream content to a receiving device 118 such as a set-top box, DVD player, game system, smart phone, television (including a smart TV), PC, a sound system receiver, a digital video recorder ("DVR"), a compact disk ("CD") device, tablet device, mobile device or other computing device or media player, and the like, allowing viewing in real time at the customer premises 116, or download it to a receiving device 118 such as a computer, DVR (also called a personal video recorder) or portable media player for viewing at any time. The program distributor 106 may offer VOD streaming, including pay-per-view and free content, whereby a user buys or selects a movie or television program and it begins to play on the presentation device 120 almost instantaneously, offer downloading of the media content to a DVR rented from the program distributor, and/or offer downloading the content onto a computer or mobile device, for viewing in the future.

In some embodiments, the receiving device 118 may be a set-top box that is typically provided by the cable provider, satellite provider, or other program distributor 106 to which the customer may subscribe to receive such on-demand services and that also receives programming through traditional channels using a terrestrial, satellite signal, and/or cable television format. However, in many embodiments, the receiving device 118 may instead be other user equipment than the set-top box such as a television, DVR, DVD player, Tablet, PC, Smart Phone or other media player not provided by or controlled by the cable provider, satellite provider, or other program distributor 106 to which the customer subscribes for such on-demand services. In such situations where the receiving device 118 is not provided by or controlled by the cable provider, satellite provider, or other program distributor 106 to which the customer subscribes for such on-demand services, it may be more difficult for the program distributor 106 to securely provide such on demand services to those devices because of the decryption which must usually occur at the

receiving device in order to present the content to the user and due to there being no unique hardware or software control of such devices by the program distributor 106 or other service provider.

Also, it may take significant processing power and time to encrypt the content differently per on-demand request and/or per user based on information received from a secure remote control device 128 associated with the user to provide the additional security and control desired. However, the systems and methods described herein for securely providing adaptive bit rate streaming media content on-demand provide solutions which overcome this difficulty and enables program distributors to more easily securely provide streaming media content to such devices, while also accommodating adaptive bit rate streaming.

In addition, information provider 138 may provide various forms of content and/or services to various devices residing in the customer premises 116. For example, Information provider 138 may also provide information to the receiving device 118 regarding insertion of advertisement or other additional content or metadata into a media content segment provided to the receiving device 118. In some embodiments, such advertisements or other additional content or metadata may be provided by an advertisement server to the content provider 104, directly to the receiving device 118 or be inserted into the streaming media stored on the content storage system of the content delivery network 122 or as it is being streamed to the receiving device 118. The information provider 138 may also or instead be another third party entity providing security data and/or services related to authentication, encryption, digital media rights, etc., on behalf of the program distributor 106 or other authorized entity.

In the illustrated example, one or more of the content provider 104, information provider 138 and/or content storage system of the content delivery network 122 may also transmit and receive additional information than the streaming media content to and from the receiving device 118 over one or

more channels within the communication system 108. For example, the content provider 104, information provider 138 and/or content storage system of the content delivery network 122 may transmit and receive indications to and from the receiving device 118 and/or secure remote control 128 regarding encryption or decryption of the streaming media content (e.g., encryption or decryption keys), information regarding differently encrypted versions of one or more same segments of a requested media content program, requests for streaming media content programs, identification of the user or user account, identification of the receiving device, authentication information, information related to digital media rights of the streaming media content, additional metadata, etc. Some or all of this additional information and metadata may also be encrypted.

For example, a user at the customer premises 116 may use the secure remote 128, which is provided to the user by the program distributor 106 or other VOD service provider, to order a VOD program via the receiving device 118 using a VOD and/or other software application running thereon. The receiving device 118 may transmit the VOD request for the ordered program to the content storage system of the content delivery network 122 or to the program distributor 106, which is then ultimately received by the content storage system of the content delivery network 122. Differently encrypted versions of particular, i.e., "special" segments of the ordered program may already be stored at the content storage system of the content delivery network 122. For example, one or more pluralities of encrypted segments may each include about one hundred encrypted versions a different corresponding "special" segment, but this number may vary and be adjusted based on desired level of security and available storage space. Each differently encrypted version of a special segment has a different decryption key which is for decrypting the corresponding differently encrypted version of that special segment. In contrast, other segments, i.e., "non-special" segments of the

requested program, are each encrypted once using the same or different encryption key from each other.

In conjunction with this request, the secure remote 128 may send a unique code associated with the secure remote 128 (and thus the user) to the content storage system of the content delivery network 122 via the receiving device 118. If the request is approved and/or authenticated by the program distributor 106 and/or the content storage system of the content delivery network 122 based on the unique code, a security server of the program distributor 106 or of the content storage system of the content delivery network 122 may then send an authorization to the secure remote 128, either directly via the communication system 108, or via the receiving device 118, such as an authorization code that allows or enables the secure remote 128 to derive the decryption key for the “non-special” segments. The content storage system of the content delivery network 122 may then begin to transmit the stored encrypted program in response to the order. The secure remote then sends this decryption key, or a portion thereof, to the receiving device 118 for decryption of those “non-special” segments. This decryption key, or the portion thereof, for decryption of those “non-special” segments may also be sent in an encrypted manner from the secure remote 128 to the receiving device.

During transmission of the ordered program, or prior thereto, once the content storage system of the content delivery network 122 encounters one of those “special segments” that have been differently encrypted a number of times and stored on the content storage system of the content delivery network 122, the content storage system of the content delivery network 122 may send a request to the program distributor 106. This request may be for information regarding which of the differently encrypted stored versions of the “special segment” of the ordered program to deliver to the receiving device 118 during the transmission of the ordered program to the receiving device 118. The program distributor 106 may then select, or have already pre-selected based on the received authorized request, which of the differently encrypted stored

versions of the “special segment” of the ordered program to deliver to the receiving device 118 during the transmission of the ordered program based on a random or pseudo-random selection process. This may also be based on the particular request or order for the streaming media content program, such as by performing the random or pseudo-random selection process per request for the program based on an identifier of the request associated with the remote control device 128. In this manner, the selection of which of the differently encrypted stored versions of the “special segment” of the ordered program to deliver is based on the current session, i.e., current request and associated transmission, for the requested program.

The secure remote 128 then sends to the receiving device 118 the correct decryption key for the receiving device 118 to decrypt the particular encrypted version selected of the “special segment” to be sent to the receiving device 118. The secure remote 128 may have pre-stored corresponding encryption and/or decryption keys and/or corresponding encryption algorithms and information associating which of these correspond with each of the differently encrypted versions of the “special” segment(s). Thus, in one embodiment, the secure remote 128 may select the applicable decryption key based on the program distributor 106 and/or the content storage system of the content delivery network communicating to the secure remote control 128 an identifier of which of the differently encrypted versions of the “special segment” of the ordered program was selected to be delivered in response to the current request or session. Alternatively, the secure remote 128 may also track what the current request is based on the program having been ordered using the secure remote 128 and use the same random or pseudo-random selection algorithm used by the program distributor 106 or the content storage system of the content delivery network 112 to determine which of the differently encrypted versions of the “special segment” of the ordered program is to be delivered from the content storage system of the content delivery network 122 to the receiving device 118 based on the current request or session. The secure remote 128

may then select from the decryption keys pre-stored in the secure remote associated with each differently encrypted version of the “special segment” accordingly.

In some embodiments, the current request may be identified by or associated with an identifier that is communicated to the receiving device 118 from the program distributor 106 or content storage system of the content delivery network 122, which is in turn displayed on the presentation device 120 with a prompt for the user to enter this identifier or select some sequence of numbers and buttons on the secure remote based on this identifier. This identifier, for example, is the same identifier based on which the program distributor 106 or the content storage system of the content delivery network 122 selected which differently encrypted version of the “special segment” of the ordered program to deliver to the receiving device 118 during transmission of the requested program. Therefore, using this same identifier and random or pseudo-random selection algorithm, the secure remote 128 can then determine which of the differently encrypted versions of the “special segment” of the ordered program was or will be selected for delivery to the receiving device 118 in response to the current request corresponding to the current session.

In this manner, different encrypted versions of the streaming media program need not be generated upon each request for the program and thus, processing time for encrypting the program for each request is saved while also providing the added security benefit of delivering a different encrypted version of “special” program segments per each request. This hinders potential content pirates from easily obtaining the required decryption key or keys for subsequent orders of the program because they would have to order the same program over and over again a number of times relative to how many times as each “special segment” of the program is differently encrypted in an attempt to intercept all the possible decryption keys.

In one example embodiment, the differently encrypted “special segments” stored in the content storage system of the content delivery network

122 represent a certain total amount (e.g., a pre-determined percentage such as 10% or 20%, etc., of the total requested program) of streaming media content programs available on-demand and are encrypted using a unique encryption key, contribution key, partial key and/or pseudo-random number stored in or derived by the secure remote 128 as described herein. For example, the differently encrypted "special segments" stored in the content storage system of the content delivery network 122 may each represent two second segments of the requested program and may appear dispersed between "non-special" encrypted segments of the requested program, but other time intervals and/or corresponding segment sizes may be used. These "non-special" encrypted segments of the requested program may have been encrypted using one encryption key common to one or more of the "non-special" encrypted segments, which are stored on or derived by the secure remote 128 based on various factors which have been previously communicated to or otherwise may be known by the secure remote 128. For example, these various factors may include communication of an authorization code communicated from the program distributor 106 and/or content storage system of the content delivery network 122.

In some embodiments, at least some of the differently encrypted versions are encrypted versions of the same segment at different bit rates. The content storage system of the content delivery network 122 may deliver an encrypted version of the segment according to a bit rate selected to enable the receiving device 118 to receive the encrypted segment at the bit rate selected based on a varying bit rate for transmission of the streaming media content program to the first remote receiving device. This may be based on the current request of the streaming media program or session corresponding to the current request. In some embodiments, the differently encrypted versions include about one hundred encrypted versions of the same segment at each of the different bit rates, but this number may vary and be adjusted according to the level of security desired. In this way, the bit rate may be changed during

transmission to the receiving device 118 dynamically according to current network conditions, receiving device 118 and/or presentation device 120 requirements, and other factors affecting bit rate.

As mentioned above, in various different embodiments, the content provider 104, information provider 138 and/or content storage system of the content delivery network 122 may transmit and receive indications to and from the receiving device 118 and/or secure remote control 128 regarding encryption or decryption of the streaming media content (e.g., encryption or decryption keys), information regarding differently encrypted versions of one or more same segments of a requested media content program, requests for streaming media content programs, identification of the user or user account, identification of the receiving device, authentication information, information related to digital media rights of the streaming media content, additional metadata, etc. Some or all of this additional information and metadata may also be encrypted. Thus, in another alternative embodiments, a server of the program distributor 106, content provider 104, information provider 138 and/or a secure server of another entity may perform the function of a relay server that selects which of the "special segments" to retrieve when encountered by the receiving device or content storage system of the content delivery network 122.

For example, the client (e.g., the receiving device 118) sends a request for a "special segment" to the relay server over the Internet via a uniform resource locator (URL). The relay server then selects, or has already pre-selected based on an initial received authorized request, which of the differently encrypted stored versions of the "special segment" of the ordered program to deliver based on a random or pseudo-random selection process. The relay server then requests that stored segment (e.g., using the random or pseudo-random number to identify the stored segment) from the content storage system of the content delivery network 122 and relays that special segment to the client. In this way, the content storage system of the content delivery network 122 does not need to know or otherwise have information

regarding what is occurring with respect to delivery of the special segment to a particular client. Also, for increased security, the relay server may translate the URL requested to a different format understood by the content storage system of the content delivery network 122, but unknown to the client, so that the client does not know where to retrieve those “special segments” off of the content storage system of the content delivery network 122.

Encryption and decryption described herein may be performed as applicable according to one or more of any number of currently available or subsequently developed encryption methods, processes, standards and/or algorithms including, but not limited to: encryption processes utilizing a public-key infrastructure (PKI), encryption processes utilizing digital certificates, the Data Encryption Standard (DES), the Advanced Encryption Standard (AES 128, AES 192, AES 256, etc.), the Common Scrambling Algorithm (CSA), encryption algorithms supporting Transport Layer Security 1.0, 1.1, and/or 1.2, encryption algorithms supporting the Extended Validation (EV) Certificate, etc.

The above description of the content distribution environment 102, the customer premises 116, and the various devices therein, is intended as a broad, non-limiting overview of an example environment in which various embodiments of securely providing adaptive bit rate streaming media content on-demand may be implemented. Figure 1 illustrates just one example of a content distribution environment 102 and the various embodiments discussed herein are not limited to such environments. In particular, content distribution environment 102 and the various devices therein, may contain other devices, systems and/or media not specifically described herein.

Example embodiments described herein provide applications, tools, data structures and other support to implement securely providing adaptive bit rate streaming media content on-demand. Other embodiments of the described techniques may be used for other purposes, including securely providing adaptive bit rate streaming media content on-demand to be played on various other receiving devices, such as audio and DVD players, digital

recorders, computers, peripherals, televisions, mobile devices, telephones, and other electronic devices, etc. In the following description, numerous specific details are set forth, such as data formats, program sequences, processes, and the like, in order to provide a thorough understanding of the described techniques. The embodiments described also can be practiced without some of the specific details described herein, or with other specific details, such as changes with respect to the ordering of the code flow, different code flows, and the like. Thus, the scope of the techniques and/or functions described are not limited by the particular order, selection, or decomposition of steps described with reference to any particular module, component, or routine.

Figure 2 is a block diagram illustrating elements of an example receiving device used in securely providing adaptive bit rate streaming media content on-demand, according to one example embodiment.

In one embodiment, the receiving device 118 is a device such as a television, DVR, DVD player, PC, tablet device, game machine, smart phone, mobile device or other computing device or media player configured to receive and process streaming media content programs and to display such programming on a presentation device. In other embodiments, the receiving device 118 is a set-top box configured to receive, process and display on a presentation device streaming media content programs and/or other programming such as cable or satellite television broadcasts via various other physical and logical channels of communication.

Note that one or more general purpose or special purpose computing systems/devices may be used to operate the receiving device 118; store information regarding the receiving device 118, store metadata, perform DRM and key management operations, decrypt received content; and communicate with the content provider 104, secure remote 128, program distributor 106, information provider 138 and/or content storage system of the content delivery network 122. In addition, the receiving device 118 may comprise one or more distinct computing systems/devices and may span

distributed locations. Furthermore, each block shown may represent one or more such blocks as appropriate to a specific embodiment or may be combined with other blocks. Also, the receiving device operation manager 222 may be implemented in software, hardware, firmware, or in some combination to achieve the capabilities described herein.

In the embodiment shown, receiving device 118 comprises a computer memory ("memory") 201, a display 202 (including, but not limited to a light emitting diode (LED) panel, cathode ray tube (CRT) display, liquid crystal display (LCD), touch screen display, etc.), one or more Central Processing Units ("CPU") 203, Input/Output devices 204 (*e.g.*, keyboard, mouse, RF or infrared receiver, universal serial bus (USB) ports, other communication ports, and the like), other computer-readable media 205, and network connections 206. The receiving device operation manager 222 is shown residing in memory 201. In other embodiments, some portion of the contents and some, or all, of the components of the receiving device operation manager 222 may be stored on and/or transmitted over the other computer-readable media 205. The components of the receiving device 118 and operation manager 222 preferably execute on one or more CPUs 203 and facilitate the receiving, decrypting, decoding, processing, selecting, recording, playback and displaying of programming, as described herein. The receiving device operation manager 222 may also facilitate on-demand media services (*e.g.*, VOD services), on-demand program ordering, processing and DRM and key management and storage corresponding to processing received streaming media content and other programming. The receiving device operation manager 222 may operate as, be part of, or work in conjunction and/or cooperation with various on-demand service software applications stored in memory 201. The receiving device operation manager 222 also facilitates communication with peripheral devices and the secure remote 128, via the I/O devices 204 and with remote systems (*e.g.*, the content provider 104, the content storage system of the

content delivery network 122, the program distributor 106, and/or the information provider 138) via the network connections 206.

Recorded or buffered programming received as streaming media content or other types of programming may reside on the media content storage 215, either in decrypted or encrypted form as applicable for securely storing, processing and displaying of the received media content according to the applicable DRM associated with the particular programming. The media content storage 215 may also store various program metadata associated with the recorded or buffered programming stored in the media content storage 215, such as that including, but not limited to, DRM data, tags, codes, identifiers, format indicators, timestamps, user identifications, authorization codes, digital signatures, etc.

The DRM and key management module 228 is configured to store decryption keys and other authorization or identification codes as applicable in a secure area of the memory 201 and enable the receiving device 118 to execute the DRM policies and rules associated with received media content. The DRM and key management module 228 may be part of or work in conjunction with various on-demand service (e.g., VOD) software applications used to enable a user to order streaming media content programs and other programming via the receiving device 118.

The media content decryption engine 226 is configured to decrypt streaming media content as it is being received by the receiving device 118 using the applicable decryption key(s) stored by the DRM and key management module according to the DRM and/or VOD software application also residing in memory 201 or other memory 230.

The graphics processing module 224 is configured to process the decrypted streaming media content and render the data for display on a particular presentation device according to specifications and requirements of the presentation device. The graphics processing module 224 may decode, decompress, format, translate, perform digital signal processing, adjust data

rate and/or complexity or perform other processing on the data representing received streaming media content as applicable for presenting the received content in real time on the presentation device as it is being received by the receiving device 118.

Other code or programs 230 (e.g., further audio/video processing modules, a program guide manager module, a Web server, and the like), and potentially other data repositories, such as data repository 220 for storing other data (user profiles, preferences and configuration data, etc.), also reside in the memory 201, and preferably execute on one or more CPUs 203. Of note, one or more of the components in Figure 2 may or may not be present in any specific implementation. For example, some embodiments may not provide other computer readable media 205 or a display 202.

In some embodiments, the receiving device 118 and operation manager 222 includes an application program interface (“API”) that provides programmatic access to one or more functions of the receiving device 118 and operation manager 222. For example, such an API may provide a programmatic interface to one or more functions of the receiving device operation manager 222 that may be invoked by one of the other programs 230, the secure remote 128, the program distributor 106, the content provider 104, information provider 138, content storage system of the content delivery network 122 or some other module. In this manner, the API may facilitate the development of third-party software, such as various different on-demand service applications, user interfaces, plug-ins, adapters (e.g., for integrating functions of the receiving device operation manager 222 and information provider 138 into desktop applications), and the like to facilitate securely providing adaptive bit rate streaming media content on-demand using the receiving device 118.

In an example embodiment, components/modules of the receiving device 118 and operation manager 222 are implemented using standard programming techniques. For example, the receiving device operation

manager 222 may be implemented as a “native” executable running on the CPU 203, along with one or more static or dynamic libraries. In other embodiments, the receiving device 118 and operation manager 222 may be implemented as instructions processed by a virtual machine that executes as one of the other programs 230. In general, a range of programming languages known in the art may be employed for implementing such example embodiments, including representative implementations of various programming language paradigms, including but not limited to, object-oriented (*e.g.*, Java, C++, C#, Visual Basic.NET, Smalltalk, and the like), functional (*e.g.*, ML, Lisp, Scheme, and the like), procedural (*e.g.*, C, Pascal, Ada, Modula, and the like), scripting (*e.g.*, Perl, Ruby, Python, JavaScript, VBScript, and the like), or declarative (*e.g.*, SQL, Prolog, and the like).

In a software or firmware implementation, instructions stored in a memory configure, when executed, one or more processors of the receiving device 118 to perform the functions of the receiving device operation manager 222. In one embodiment, instructions cause the CPU 203 or some other processor, such as an I/O controller/processor, to receive decryption keys, access codes, identifications codes, etc., from external devices such as wirelessly from the secure remote 128 or other external secure device, and to decrypt or descramble such received information as applicable and transmit one or more of such codes with or in conjunction with transmitting a request for a streaming media program to a remote system according to on-demand service software applications running on the receiving device 118. The instructions cause the CPU 203 or some other processor, such as an I/O controller/processor, to receive, decrypt and process the requested streaming media program for display on a presentation device using the received decryption key.

The embodiments described above may also use well-known or other synchronous or asynchronous client-server computing techniques. However, the various components may be implemented using more monolithic

programming techniques as well, for example, as an executable running on a single CPU computer system, or alternatively decomposed using a variety of structuring techniques known in the art, including but not limited to, multiprogramming, multithreading, client-server, or peer-to-peer (e.g., Bluetooth® wireless technology providing a communication channel between the receiving device 118 and the secure remote 128), running on one or more computer systems each having one or more CPUs or other processors. Some embodiments may execute concurrently and asynchronously, and communicate using message passing techniques. Equivalent synchronous embodiments are also supported by a receiving device operation manager 222 implementation. Also, other functions could be implemented and/or performed by each component/module, and in different orders, and by different components/modules, yet still achieve the functions of the receiving device 118 and operation manager 222.

In addition, programming interfaces to the data stored as part of the receiving device 118 and operation manager 222, can be available by standard mechanisms such as through C, C++, C#, and Java APIs; libraries for accessing files, databases, or other data repositories; scripting languages such as XML; or Web servers, FTP servers, or other types of servers providing access to stored data. The media content storage 216 and other data 220 may be implemented as one or more database systems, file systems, or any other technique for storing such information, or any combination of the above, including implementations using distributed computing techniques.

Different configurations and locations of programs and data are contemplated for use with techniques described herein. A variety of distributed computing techniques are appropriate for implementing the components of the illustrated embodiments in a distributed manner including but not limited to TCP/IP sockets, RPC, RMI, HTTP, and Web Services (XML-RPC, JAX-RPC, SOAP, and the like). Other variations are possible. Other functionality could also be provided by each component/module, or existing functionality could be

distributed amongst the components/modules in different ways, yet still achieve the functions of the receiving device operation manager 222.

Furthermore, in some embodiments, some or all of the components of the receiving device 118 and operation manager 222 may be implemented or provided in other manners, such as at least partially in firmware and/or hardware, including, but not limited to one or more application-specific integrated circuits (“ASICs”), standard integrated circuits, controllers (e.g., by executing appropriate instructions, and including microcontrollers and/or embedded controllers), field-programmable gate arrays (“FPGAs”), complex programmable logic devices (“CPLDs”), and the like. Some or all of the system components and/or data structures may also be stored as contents (e.g., as executable or other machine-readable software instructions or structured data) on a computer-readable medium (e.g., as a hard disk; a memory; a computer network, cellular wireless network or other data transmission medium; or a portable media article to be read by an appropriate drive or via an appropriate connection, such as a DVD or flash memory device) so as to enable or configure the computer-readable medium and/or one or more associated computing systems or devices to execute or otherwise use, or provide the contents to perform, at least some of the described techniques.

Figure 3 is a block diagram of an example content storage system of a content delivery network 122 in operable communication with multiple remote example receiving devices 118a to 118n such as that of Figure 2 to which streaming media content is securely provided on-demand, according to one example embodiment.

In one embodiment, the receiving devices 118a to 118n are not controlled or provided by the program distributor 106 or other entity providing the on-demand service via the content storage system of the content delivery network 122. For example, receiving devices 118a to 118n may be any combination of Internet connected televisions, DVRs, DVD players, PCs, tablet devices, game machines, smart phones, mobile devices or other computing

devices or media players not controlled or provided by the program distributor 106 or other entity providing the on-demand service via the content storage system of the content delivery network 122. However, each receiving device 118a to 118n may request the same or different streaming media content (stored at the content storage system of the content delivery network 122) on-demand using VOD or other available on-demand services and/or applications associated with, in communication with or running on the respective receiving devices 118a to 118n. In response, the content storage system of the content delivery network 122 will deliver the requested content uniquely for each received request (e.g., according to selections of stored differently encrypted special segments of the requested program that are unique for each request) and deliver the encrypted requested content to the appropriate respective receiving device of the receiving devices 118a to 118n. The respective receiving devices 118a to 118n will then each decrypt the streaming content as it is being received and cause it to be displayed according to the corresponding decryption key communicated from the respective individual remote 128a to 128n to the respective receiving device 118a to 118n in conjunction with the respective request.

For example, the user at customer premises 116a may use their individual secure remote 128a that was provided by the program distributor to order a movie on-demand to be delivered as streaming content to their respective receiving device 118a (e.g., their Internet-connected television) via communication system 108. The user selects the movie using their secure remote 128a from an electronic program guide (EPG) displayed on their television by pressing a button on their secure remote 128a. In response to pressing on this button, the secure remote then communicates an identification code (which may in many instances be sent in the clear or unencrypted manner) wirelessly to the receiving device 118a. However, the code may be otherwise transmitted by the secure remote 128a to the receiving device 118a in conjunction with the user operating the remote 128a to order the movie, such

as by pressing a special designated button on the secure remote 128a different than that used to select the movie and/or a button pressed in response to a prompt displayed on the EPG.

The code may be provided wirelessly by the secure remote 128a to the receiving device 118a, such that the receiving device 118a can then transmit the code to the content storage system of the content delivery network 122 and/or program distributor 106 when the request for the streaming media content program is transmitted by the receiving device 118. In one embodiment, this unique code is unique to the secure remote 128a and may be pre-programmed and stored in the secure remote 128a (which may be manufactured, controlled, modified and/or provided to the user by the program distributor 106 or other entity providing or making available the on-demand service). The secure remote 128a is provided to the user who is uniquely associated with that code, and thus also the secure remote 128a, for authentication purposes to order the VOD programming.

Once the content storage system of the content delivery network 122 and/or program distributor 106 authenticates the request, such as by using the received code to associate the request with an authorized user or identifier of an authorized user, the content storage system of the content delivery network 122 may deliver the requested program and particular differently encrypted special segments as instructed by the program distributor 106 in response to a request from the Content Deliver Network 122.

In some embodiments, the authentication may occur at the receiving device 118a such that the receiving device 118a does not allow the request to be sent from the receiving device 118a, or the content may not be decrypted by the receiving device 118a unless and until the receiving device 118a authenticates or receives notice of authentication using the code received from the secure remote 128a in conjunction with VOD application software running on the receiving device 118. On other embodiments, the authentication may occur directly between the secure remote 128 and the content storage

system of the content delivery network 122 and/or the program distributor 106 over the communication system 108, such as when the secure remote 128 is a smart phone or other wireless device with Wi-Fi® capability and the authentication occurs over the cellular telephone network or computer network such as the Internet.

In some embodiments, only particular streaming media content programs of all those available on-demand and/or only portions (e.g., a pre-determined percentage such as 10% or 20%) of streaming media content programs available on-demand have associated segments differently encrypted using different unique encryption/decryption key pairs known or derived by the secure remote 128 as described herein. For example, this may be to provide additional security for particular higher value content, to allocate systems resources more efficiently and/or for other reasons as desirable by the program distributor 106 because the content storage system of the content delivery network 122 need not uniquely encrypt content upon each request.

Figure 4 is a block diagram illustrating components of an example embodiment of a secure remote-control device 128 used in securely providing adaptive bit rate streaming media content on-demand in wireless communication with a receiving device 118, according to one example embodiment.

In the embodiment shown, secure remote 128 comprises a computer memory (“memory”) 401, a display 402, one or more Central Processing Units (“CPU”) 403, other Input/Output devices 404 (e.g., keyboard, wheel input, touch pad), other computer-readable media 405 (e.g., flash memory, SIM card), and network connections 406. The display 402 may be, for example a bit-mapped LCD display, having sufficient resolution to display multiple lines of text and/or other user interface elements. The network connections 406 include one or more communication interfaces to various media devices, including but not limited to radio frequency transceivers, infrared transceivers, wireless Ethernet (“Wi-Fi”) interfaces, and the like.

The secure remote 128 communicates with receiving device 118. The receiving device 118 may be a media device, television or any other device amenable to control by the secure remote 128. Example media devices include other remote-control devices, video recorders, audio systems, televisions, displays, personal computers, set-top boxes, mobile devices, and the like.

Secure remote logic 410 and device information 411 is shown residing in memory 401. In other embodiments, some portion of the contents, some of, or all of the components of the logic 410 may be stored on and/or transmitted over the other computer-readable media 405. The logic 410 preferably executes on one or more CPUs 403 and manages the secure remote 128, as described herein. Other code or programs and potentially other data/information (not shown), may also reside in the memory 401, and preferably execute on one or more CPUs 403. Of note, one or more of the components in Figure 4 may not be present in any specific implementation. For example, some embodiments may not provide other computer readable media 405 and network connections 406.

The logic 410 performs the core functions of the secure remote 128 for controlling the receiving device 118 and also those functions as discussed with respect to Figure 1 through Figure 3 above. In particular, the logic 410 causes the appropriate decryption key or appropriate part of the decryption key to be sent to the receiving device 118 at the applicable time such that ordered streaming media content (such as that ordered using the secure remote 128) may be decrypted by the receiving device 118.

The secure remote 128 sends to the receiving device 118 the correct decryption key for the receiving device 118 to decrypt the particular encrypted version selected of the "special segment" to be sent to the receiving device 118. The secure remote 128 may have pre-stored corresponding encryption and/or decryption keys and/or corresponding encryption algorithms and information associating which of these correspond with each of the differently encrypted versions of the "special" segment(s) of the requested

program. Such information may be stored in the protected memory 416 and/or implemented by the security logic 414 as applicable of the secure smart card 412.

Thus, in one embodiment, the secure remote 128 may use the security logic 414 to select the applicable decryption key based on the program distributor 106 and/or the content storage system of the content delivery network communicating to the secure remote control 128 an identifier of which of the differently encrypted versions of the "special segment" of the ordered program was selected by the program distributor 106 or the content storage system of the content delivery network 122 to be delivered in response to the current request or session. Alternatively, the secure remote 128 may also track what the current request is based on the program having been ordered using the secure remote 128 and use the same random or pseudo-random selection algorithm used by the program distributor 106 or the content storage system of the content delivery network 112 to determine which of the differently encrypted versions of the "special segment" of the ordered program is to be delivered from the content storage system of the content delivery network 122 to the receiving device 118 based on the current request or session. The secure remote 128 may then select from the decryption keys pre-stored in the secure remote associated with each differently encrypted versions of the "special segment" accordingly.

The respective receiving devices will then each decrypt the streaming content as it is being received according to the corresponding decryption key, part of a decryption key, contribution key or pseudo random number, communicated from the respective individual secure remote 128 to the respective receiving device 118 in conjunction with the respective request for the content.

In the present example embodiment, the secure remote 128 stores the decryption keys (or part of the decryption key) in a secure protected memory area 416 such as in a secure smart card 412 within the secure remote

128 needed to decrypt the one or more differently encrypted special segments received by the receiving device 118 from the content storage system of the content delivery network 122. For example, the security logic 414 stored on the secure smart card 412 may cause this decryption key to be selected according to the same encryption/decryption key pair generation algorithm associated with the particular differently encrypted "special segment" selected by the program distributor 106 or content storage system of the content delivery network 122 and used by the content storage system of the content delivery network 122 for the particular selected "special segment". This associated the same encryption/decryption key pair generation algorithm may also be stored in the protected memory 416 of the secure remote 128 along with the algorithm of how a particular differently encrypted "special segment" is selected based on a current request for the selection program or based on a unique identifier of the current request. Also, security logic 414 may be implemented using obfuscated code techniques, which is obfuscating computer program code (e.g., writing or generating the program code in a manner such that it is difficult for humans to understand) to conceal its purpose or its logic. This increases security by aiding in the prevention of tampering and deterring reverse engineering to gain access to the decryption key or other secret or sensitive data. The security logic 414 could also be fully or partially implemented using white box cryptography (WBC). For example, white box cryptography may use a special purpose code generator that turns a given cipher into a robust representation where the operations on the secret key are combined with random data and code in such a way that the random data cannot be distinguished from key information. In various embodiments, the security logic 414 may be hardware or software based, smart card based, or implemented using removable devices such as Secure Digital (SD) memory cards, secure personal information manager/management systems (PIMS) such as in cell phones, USB security devices, etc.

The secure remote 128 may send the stored corresponding decryption key to the receiving device 118 in response to a user selection of a button of the I/O devices 404 or other selection of an input selection item of the I/O devices 404 on the secure remote 128. The user may be prompted by the VOD application software on the receiving device 118 or other program guide displayed on the presentation device 120 to send the decryption key using the secure remote 128 at the appropriate time during the VOD ordering process, or to enter a request code or authorization code communicated via the receiving device 118 to the user based on the received current request. However, if the secure remote 128 is a two-way communication device such that it can receive communication signals from the receiving device 118, such as via the I/O devices 404 and/or network connections 406, the receiving device 118 may indicate automatically to the secure remote 128 when to transmit the decryption key and the secure remote 128 will then automatically transmit the decryption key accordingly. In some embodiments, each time the secure remote 128 automatically transmits the decryption code, it will signal an encrypted segment selection algorithm to generate the next request identifier or code in the sequence in preparation for determining what the next differently encrypted segment selection(s) will be for the next request. Alternatively, the two-way secure remote 128 may determine what the next encrypted segment selection(s) in the sequence will be upon receiving a new request from the receiving device 118 to transmit the decryption key, or may just receive this information via the network connections 406 from the security server of the content storage system of the content delivery network 122 or program distributor 106 if such are available in the secure remote 128.

In an example embodiment, the logic 410 and security logic 414 are implemented using standard programming techniques. For example, the logic 410 may be implemented as a "native" executable running on the CPU 403, along with one or more static or dynamic libraries. In other embodiments, the logic 410 may be implemented as instructions processed by a virtual

machine that executes as some other program. In general, a range of programming languages known in the art may be employed for implementing such example embodiments, including representative implementations of various programming language paradigms, including but not limited to, object-oriented (*e.g.*, Java, C++, C#, Visual Basic.NET, Smalltalk, and the like), functional (*e.g.*, ML, Lisp, Scheme, and the like), procedural (*e.g.*, C, Pascal, Ada, Modula, and the like), scripting (*e.g.*, Perl, Ruby, Python, JavaScript, VBScript, and the like), declarative (*e.g.*, SQL, Prolog, and the like).

Also, security logic 414 could be implemented using obfuscated code techniques, which is obfuscating computer program code (*e.g.*, writing or generating the program code in a manner such that it is difficult for humans to understand) to conceal its purpose or its logic. This increases security by aiding in the prevention of tampering and deterring reverse engineering to gain access to the decryption key or other secret or sensitive data. The security logic 414 could also be fully or partially implemented using white box cryptography (WBC). For example, white box cryptography may use a special purpose code generator that turns a given cipher into a robust representation where the operations on the secret key are combined with random data and code in such a way that the random data cannot be distinguished from key information. The security logic 414 may be hardware or software based, smart card based, or implemented using removable devices such as Secure Digital (SD) memory cards, secure personal information manager/management systems (PIMS) such as in cell phones, USB security devices, etc.

The embodiments described above may also use well-known or proprietary synchronous or asynchronous client-server computing techniques. However, the various components may be implemented using more monolithic programming techniques as well, for example, as an executable running on a single CPU computer system, or alternatively decomposed using a variety of structuring techniques known in the art, including but not limited to, multiprogramming, multithreading, client-server, or peer-to-peer, running on one

or more computer systems each having one or more CPUs. Some embodiments may execute concurrently and asynchronously, and communicate using message passing techniques. Equivalent synchronous embodiments are also supported. Also, other functions could be implemented and/or performed by each component/module, and in different orders, and by different components/modules, yet still achieve the functions of the smart remote.

In addition, programming interfaces to the data stored as part of the device information 411, can be available by standard mechanisms such as through C, C++, C#, and Java APIs; libraries for accessing files, databases, or other data repositories; through scripting languages such as XML; or through Web servers, FTP servers, or other types of servers providing access to stored data. The device information 411 may be implemented as one or more database systems, file systems, or any other technique for storing such information, or any combination of the above, including implementations using distributed computing techniques.

Different configurations and locations of programs and data are contemplated for use with techniques of described herein. A variety of distributed computing techniques are appropriate for implementing the components of the illustrated embodiments in a distributed manner including but not limited to TCP/IP sockets, RPC, RMI, HTTP, Web Services (XML-RPC, JAX-RPC, SOAP, and the like). Other variations are possible. Also, other functionality could be provided by each component/module, or existing functionality could be distributed amongst the components/modules in different ways, yet still achieve the functions of an HDM.

Furthermore, in some embodiments, some or all of the components/portions of the logic 410 and security logic 414 may be implemented or provided in other manners, such as at least partially in firmware and/or hardware, including, but not limited to one or more application-specific integrated circuits ("ASICs"), standard integrated circuits, controllers (e.g., by executing appropriate instructions, and including microcontrollers and/or

embedded controllers), field-programmable gate arrays (“FPGAs”), complex programmable logic devices (“CPLDs”), and the like. Some or all of the system components and/or data structures may also be stored as contents (e.g., as executable or other machine-readable software instructions or structured data) on a computer-readable medium (e.g., as a hard disk; a memory; a computer network or cellular wireless network or other data transmission medium; or a portable media article to be read by an appropriate drive or via an appropriate connection, such as a DVD or flash memory device) so as to enable or configure the computer-readable medium and/or one or more associated computing systems or devices to execute or otherwise use or provide the contents to perform at least some of the described techniques. Such computer program products may also take other forms in other embodiments. Accordingly, embodiments of the secure remote include other configurations. For example, the secure remote 128 may be, but is not limited to being, one or any combination of the following devices which may have a hardware or software security element: a mobile device (e.g., a smart phone or tablet device), a wireless device, a wireless device configured for two-way communication, a short range wireless device, a wireless device configured to use radio frequency wireless transmissions, a wireless device configured to use short-wave wireless transmissions, a wireless device configured to use infrared wireless transmissions, a wireless device configured to use sonic transmissions, a consumer electronics remote control device, an entertainment system remote control device, a universal remote control device, a set-top box remote control device, a television remote control device, a mobile telephone, a key fob, a universal serial bus a (USB) device, an access card, a flash memory device, a radio frequency identification device, a near field communication device, a security token, etc.

Figure 5 is a diagram illustrating an example of how particular segments of a streaming media content program 501 may be differently encrypted a number of times and stored in a content storage system of a

content delivery network 122 in a system for securely providing adaptive bit rate streaming media content on-demand, according to one example embodiment.

In particular, shown are example segments 1 through 13 of an encrypted media content program 501 stored, for example, on content storage system of the content delivery network 122. Also shown are the stored differently encrypted versions of "special" segments 3, 7 and 11. For "special" segment 3, shown are n differently encrypted versions of segment 3 (encrypted versions 3a through 3n). For "special" segment 7, shown are n differently encrypted versions of segment 7 (encrypted versions 7a through 7n). For "special" segment 11, shown are n differently encrypted versions of segment 11 (encrypted versions 11a through 11n).

In response to a request for the streaming media content program 501, during transmission of the streaming media content program 501, or prior thereto, once the content storage system of the content delivery network 122 encounters one of those "special" segments 3, 7 or 11 that have been differently encrypted a number of times and stored on the content storage system of the content delivery network 122, the content storage system of the content delivery network 122 may send a request to the program distributor 106 for information regarding which of the differently encrypted stored versions of the "special segment" of the requested program 501 to deliver to the receiving device 118 during the transmission of the requested program 501 to the receiving device 118. For example, a security server of the program distributor 106 may randomly select segment 3c to send to the receiving device based on the current request or session associated with the current request. This will be communicated by the security server of the program distributor 106 to the content storage system of the content delivery network 122 when the content storage system of the content delivery network 122 requests which encrypted version of differently encrypted segment 3 to send. The content storage system of the content delivery network 122 will then read stored encrypted version 3c of segment 3 and send it to the receiving device 118 accordingly during

transmission of the requested program 501 in response to the request for the streaming media content program 501 received from the receiving device 118 and originating from the remote control 128. In this manner, the random or pseudo-random selection of which of the differently encrypted stored versions of the "special segment" of the ordered program to deliver is based on the current session, i.e., current request and associated transmission, for the requested program. In the present example embodiment, when the same special segment is requested during the current session, the same version of that special segment is delivered. For example, during the current session, when special segment 3 is requested, segment 3c will always be sent in response.

Figure 6 is a flow diagram of a method 600 in a security server in a media content transmission system shown in Figure 1 through Figure 4 of providing adaptive bit rate streaming media content on-demand, according to one example embodiment.

At 602, the security server of the program distributor 106 of the media content transmission system receives a request for a streaming media content program from a remote receiving device 118.

At 604, the security server of the program distributor 106 of the media content transmission system, in response to receiving the first request, authenticates the first request.

At 606, the security server of the program distributor 106 selects an encrypted segment of the requested streaming media content program, the encrypted segment being one of a first plurality of encrypted segments having been stored prior to receiving said first request for the streaming media content program, each encrypted segment of the first plurality of encrypted segments being a differently encrypted version of a same segment of the of the requested streaming media content program and having a different corresponding decryption key.

At 608, the security server of the program distributor 106 transmits one or more of: the selected encrypted segment of the requested streaming media content program and an identifier indicative of the selected encrypted segment to enable the first remote receiving device to receive the selected encrypted segment in response to the first request.

Figure 7 is a flow diagram of method 700 in a secure remote control shown in figures 1, 3 and 4, of securely providing adaptive bit rate streaming media content on-demand, according to one example embodiment.

At 702, the secure remote control 128 receives a first request for a streaming media content program, the first request originating from a first secure remote control device communicatively coupled to a first remote receiving device 118.

At 704, the secure remote control 128, in response to the received user input, transmits a first request for the streaming media content program and transmits information to enable authentication of said first request.

At 706, the secure remote control 128 determines which encrypted segment of a first plurality of encrypted segments stored within a content delivery network is for delivery to the receiving device 118 via the content delivery network in response to the first request for the streaming media content program, each of the encrypted segments being a differently encrypted version of a same segment of the requested streaming media content program and associated with a corresponding decryption key.

At 708, the secure remote control 128 transmits to the receiving device, based on the determination of which encrypted segment of the first plurality of encrypted segments is for delivery, the corresponding decryption key or part of the corresponding decryption key needed to aid in decryption of the encrypted segment of the requested streaming media content program determined to be for delivery to the receiving device 118.

Figure 8 is a flow diagram 800 of method in a content storage system of a content delivery network 122 shown in Figure 1 through Figure 4, of

securely providing adaptive bit rate streaming media content on-demand, according to one example embodiment.

At 802, the content storage system of a content delivery network 122, in response to authentication of a first request for a streaming media content program, begins to transmit the requested streaming media content program to a first remote receiving device associated with the request.

At 804, the content storage system of a content delivery network 122 requests information, by the content storage system, regarding which encrypted segment of a first plurality of stored encrypted segments of the requested streaming media content program is to be delivered by the content storage system to the first remote receiving device based on the first request for the streaming media content program.

At 806, the content storage system of a content delivery network 122, in response to the request, receives the information regarding which encrypted segment is to be delivered by the content storage system to the remote receiving device.

At 808, the content storage system of a content delivery network 122, in response to the request, delivers, based on the received information, the encrypted segment to the remote receiving device during the transmission of the requested streaming media content program to the first remote receiving device.

While various embodiments have been described herein above, it is to be appreciated that various changes in form and detail may be made without departing from the spirit and scope of the invention(s) presently or hereafter claimed.

U.S. Provisional Patent Application No. 61/779,979, filed March 13, 2013, is incorporated herein by reference, in its entirety.

CLAIMS

1. A method in a media content transmission system, the method comprising:

receiving, by a security server of the content transmission system, a first request for a streaming media content program, the first request originating from a first secure remote control device communicatively coupled to a first remote receiving device;

in response to receiving the first request, authenticating, by the security server, the first request;

selecting, by the security server, an encrypted segment of the requested streaming media content program, the encrypted segment being one of a first plurality of encrypted segments having been stored prior to receiving said first request for the streaming media content program, each encrypted segment of the first plurality of encrypted segments being a differently encrypted version of a same segment of the of the requested streaming media content program and having a different corresponding decryption key; and

transmitting, by the media content transmission system, one or more of: the selected encrypted segment of the requested streaming media content program and an identifier indicative of the selected encrypted segment to enable the first remote receiving device to receive the selected encrypted segment in response to the first request.

2. The method of claim 1 further comprising, transmitting to the first secure remote control device, by the media content transmission system, information indicative of a corresponding decryption key for the selected encrypted segment based on the received first request for the streaming media content program.

3. The method of claim 2 wherein the selected encrypted segment is selected based on a request, received from a content storage system of a content delivery network, for an identifier indicative of which encrypted segment of the first plurality of encrypted segments, based on the first request for the streaming media content program, is to be delivered by the content storage system of the content delivery network to the remote receiving device, and the transmitting includes transmitting, by the security server, the identifier indicative of the selected encrypted segment to the content storage system of the content delivery network.

4. The method of claim 3 wherein the streaming media content program, including the first plurality of encrypted segments, is stored on the content storage system of the content delivery network prior to receiving the first request, the content storage system of the content delivery network located geographically remote from the security server.

5. The method of claim 4 wherein the content storage system of the content delivery network is part of the media content transmission system.

6. The method of claim 2 wherein the information transmitted to the first secure remote control device indicative of the corresponding decryption key is information based on which the first secure remote control device can derive the decryption key.

7. The method of claim 2 wherein the information transmitted to the first secure remote control device indicative of the corresponding decryption key is an encrypted version of the corresponding decryption key or a part of the corresponding decryption key.

8. The method of claim 1 wherein the transmitting includes transmitting the identifier indicative of the selected encrypted segment to the first remote receiving device or to the first secure remote control device.

9. The method of claim 1 further comprising:

receiving, by the media content transmission system, based on the first request for the streaming media content program, a request for an identifier of an encrypted segment of the first plurality of encrypted segments of the requested streaming media content program, and wherein the transmitting includes transmitting, based on the received request for the identifier of an encrypted segment of the first plurality of encrypted segments, the identifier of the selected encrypted segment to a content storage system of a content delivery network on which the first plurality of encrypted segments is stored.

10. The method of claim 1 wherein at least some of the differently encrypted versions are encrypted versions of the same segment at different bit rates and wherein the selecting the encrypted segment of the requested streaming media content program is based on a pseudo-random selection and is further based on a bit rate selected to enable the first remote receiving device, based on the first request, to receive the selected encrypted segment at the selected bit rate based on a varying bit rate for transmission of the streaming media content program to the first remote receiving device.

11. A remote control device comprising:

a processor; and

a secure memory area coupled to the processor, wherein the processor is configured to:

receive user input indicative of a request for a streaming media content program to be transmitted a receiving device communicatively coupled to the remote control;

in response to the received user input, transmit a first request for the streaming media content program and transmit information to enable authentication of said first request;

determine which encrypted segment of a first plurality of encrypted segments stored within a content delivery network is for delivery to the receiving device via the content delivery network in response to the first request for the streaming media content program, each of the encrypted segments being a differently encrypted version of a same segment of the requested streaming media content program and associated with a corresponding decryption key; and

transmit to the receiving device, based on the determination of which encrypted segment of the first plurality of encrypted segments is for delivery, the corresponding decryption key or part of the corresponding decryption key needed to aid in decryption of the encrypted segment of the requested streaming media content program determined to be for delivery to the receiving device.

12. The remote control device of claim 11, wherein the remote control is further configured to:

receive information regarding which encrypted segment of the first plurality of encrypted segments is for delivery, and wherein the remote control device is configured to make the determination of which encrypted segment of the first plurality of encrypted segments is for delivery based on the receive information.

13. The remote control device of claim 12, wherein the received information is an identifier of which encrypted segment of the first plurality of encrypted segments is for delivery.

14. A computer-implemented method in a content storage system of a content delivery network, the method comprising:

in response to authentication of a first request for a streaming media content program, beginning, by the content storage system, to transmit the requested streaming media content program to a first remote receiving device associated with the request;

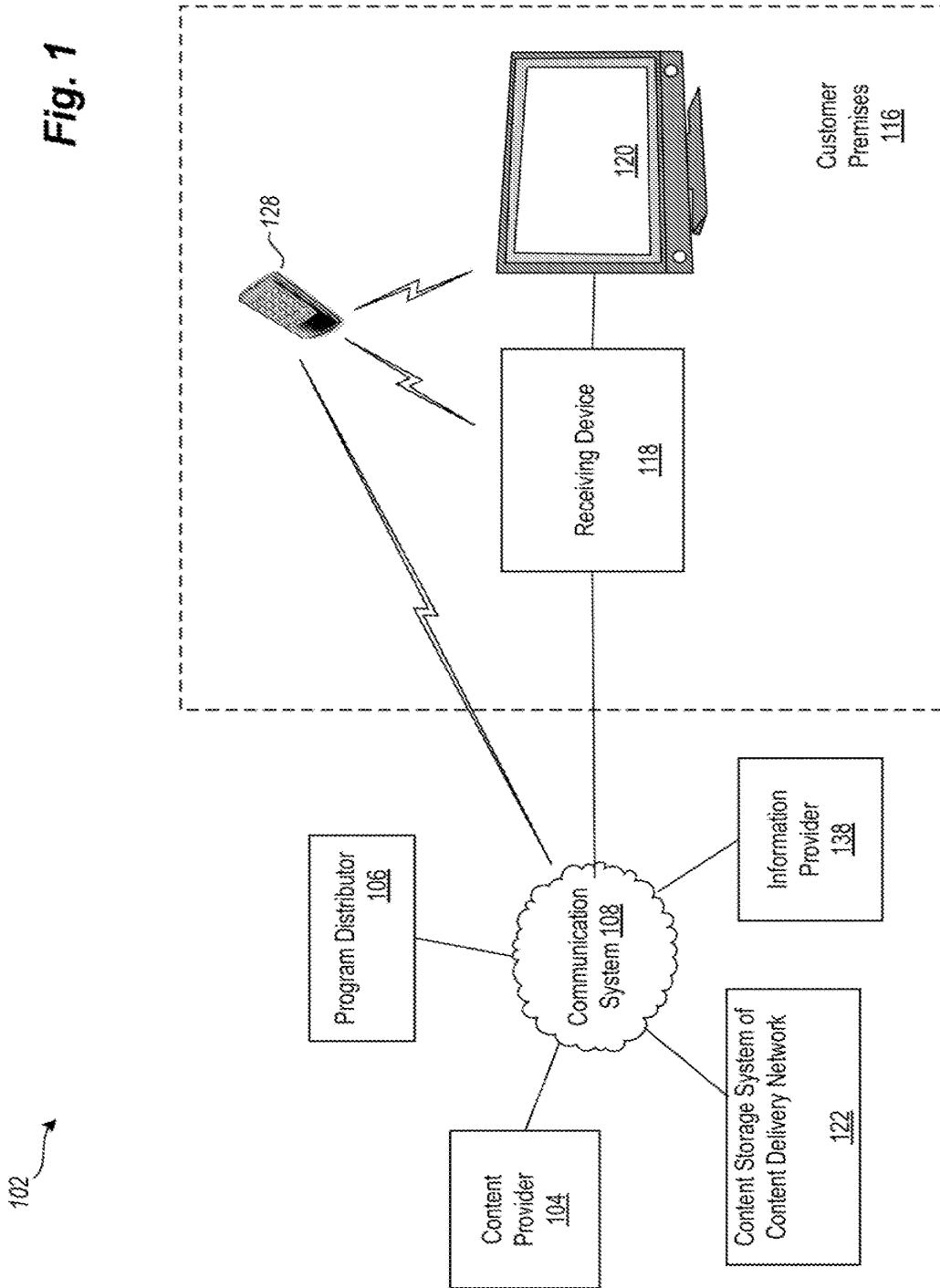
requesting information, by the content storage system, regarding which encrypted segment of a first plurality of stored encrypted segments of the requested streaming media content program is to be delivered by the content storage system to the first remote receiving device based on the first request for the streaming media content program;

in response to the request, receiving the information regarding which encrypted segment is to be delivered by the content storage system to the remote receiving device; and

delivering, by the content storage system, based on the received information, the encrypted segment to the remote receiving device during the transmission of the requested streaming media content program to the first remote receiving device.

15. The method of claim 14 wherein the requesting the information occurs before the beginning to transmit the requested streaming media content program.

Fig. 1



102 →

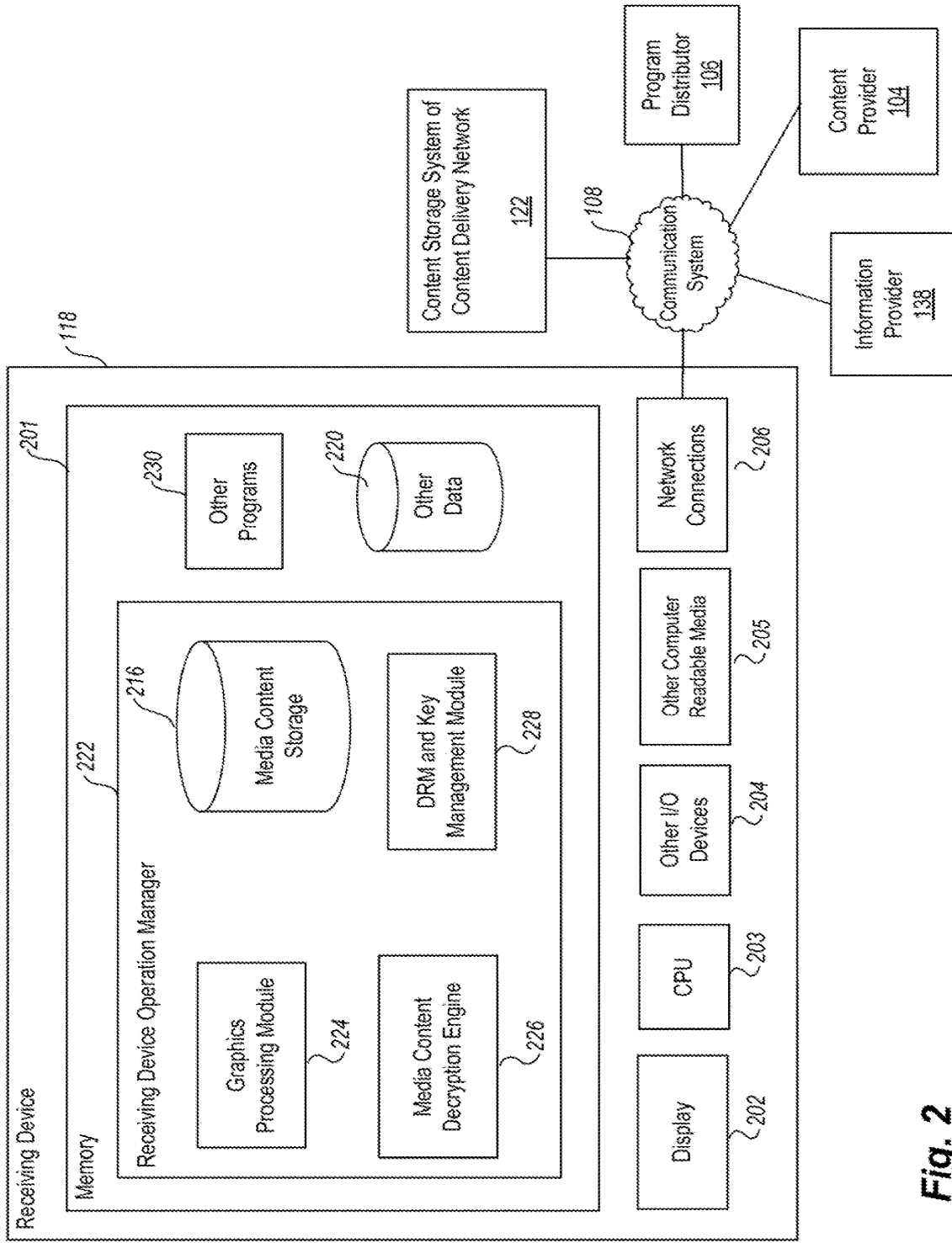


Fig. 2

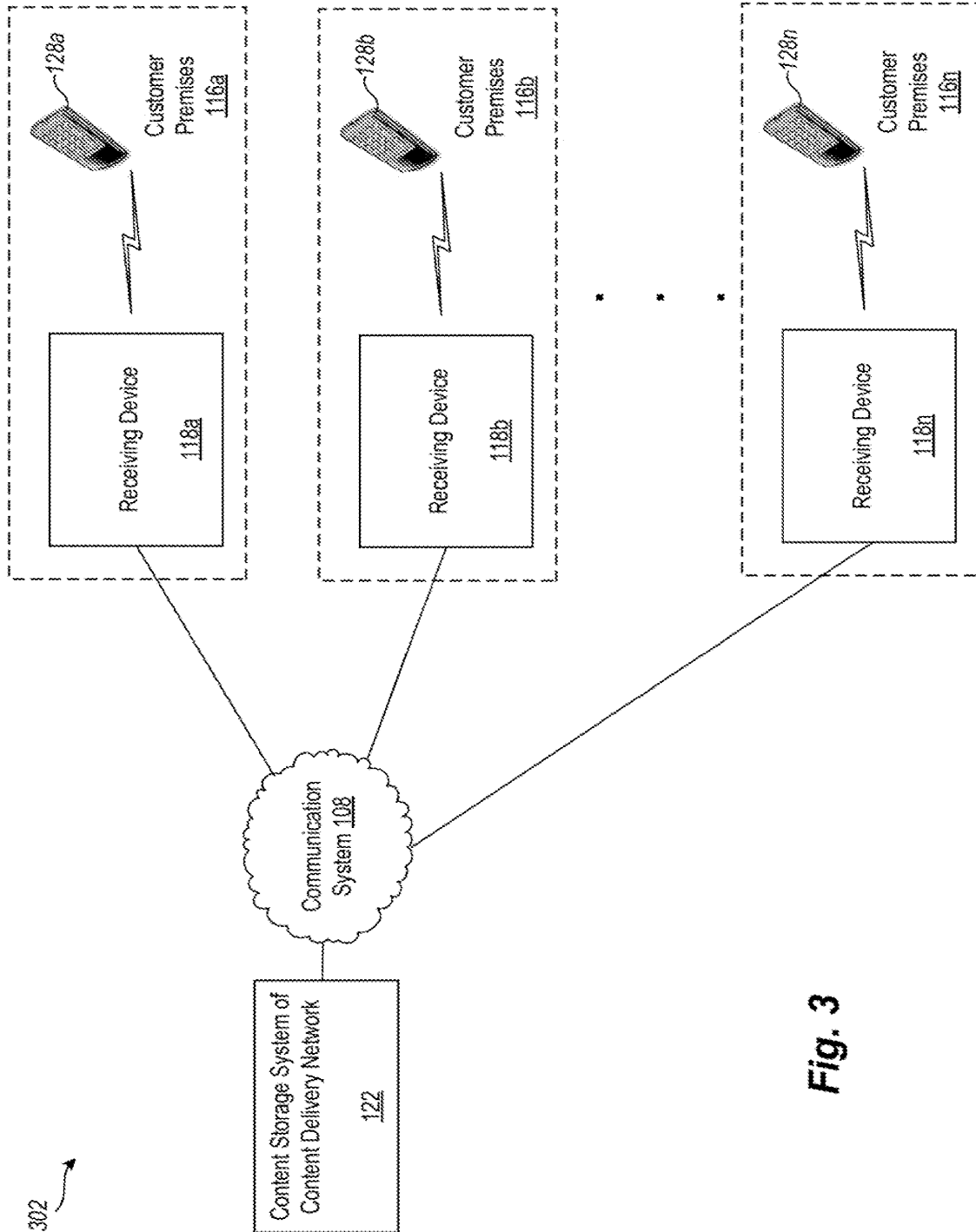


Fig. 3

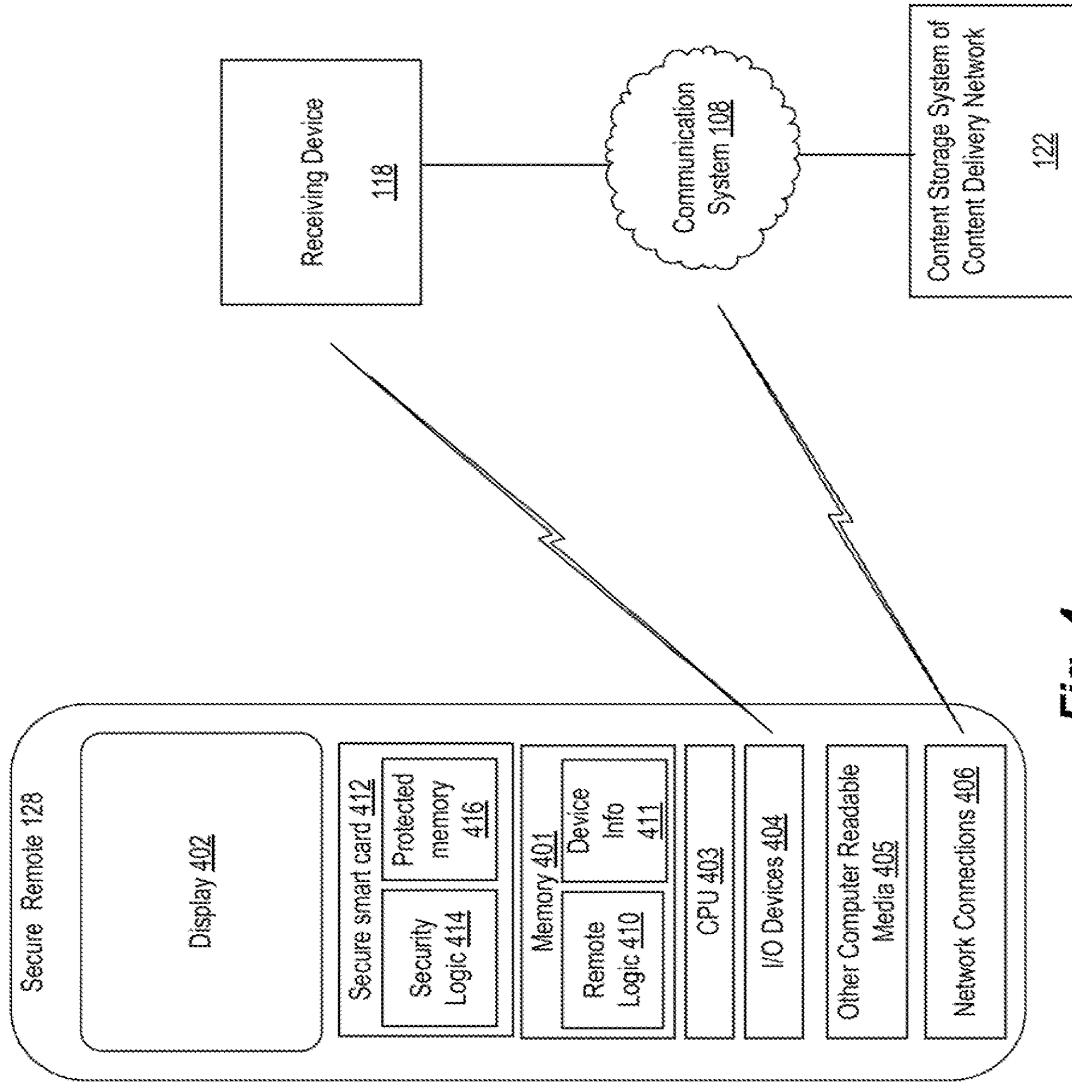


Fig. 4

Stored Encrypted Streaming Media Content Program

501

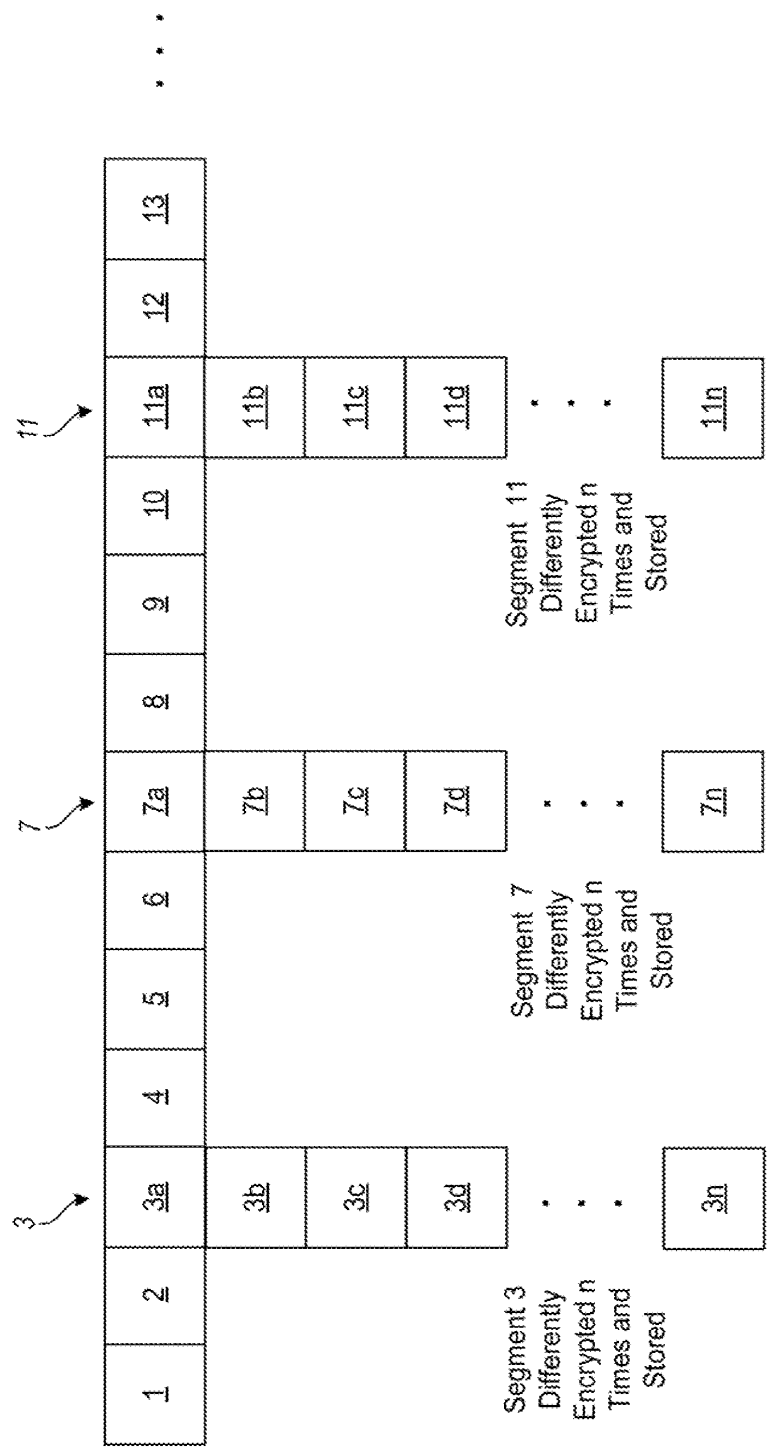


Fig. 5

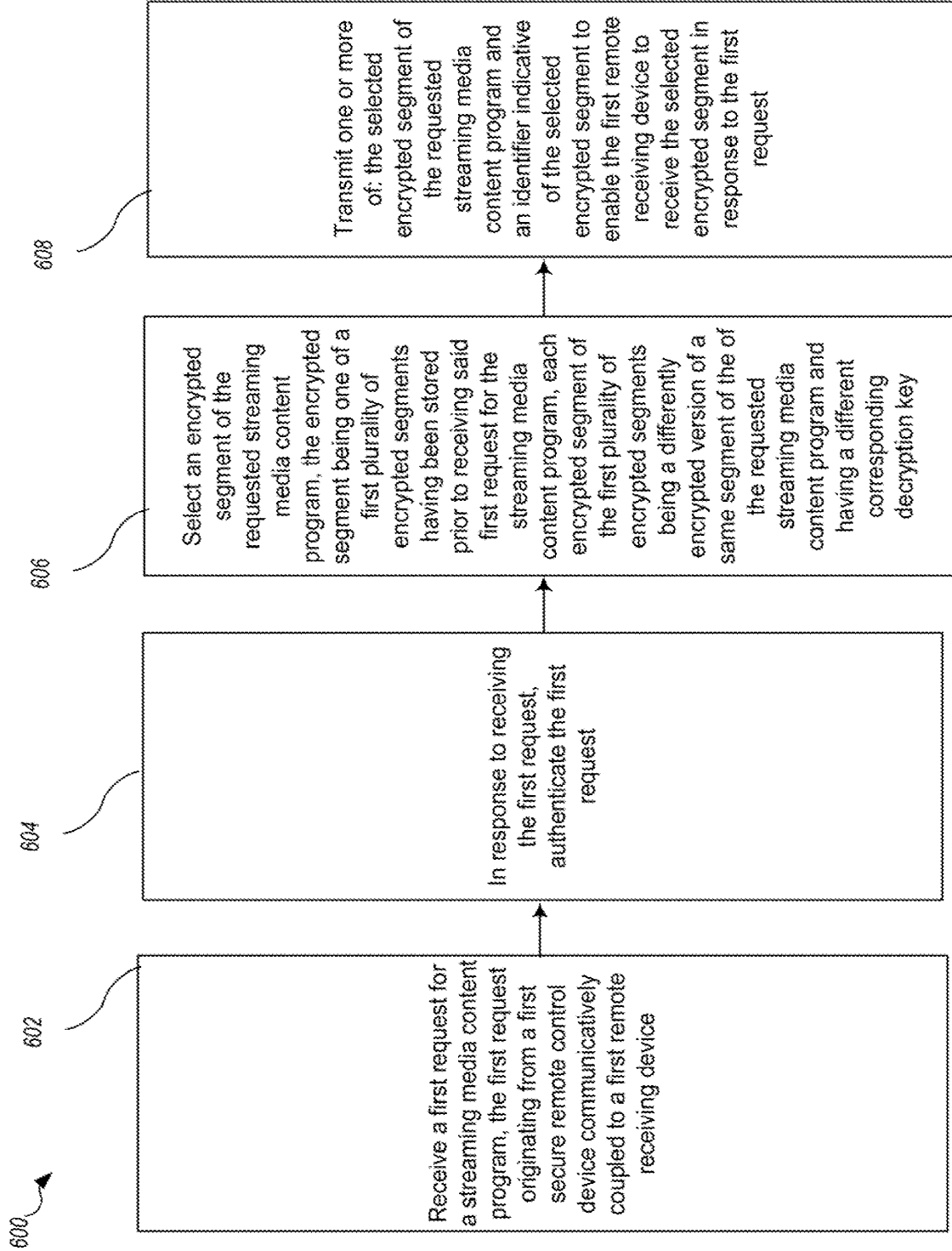


Fig. 6

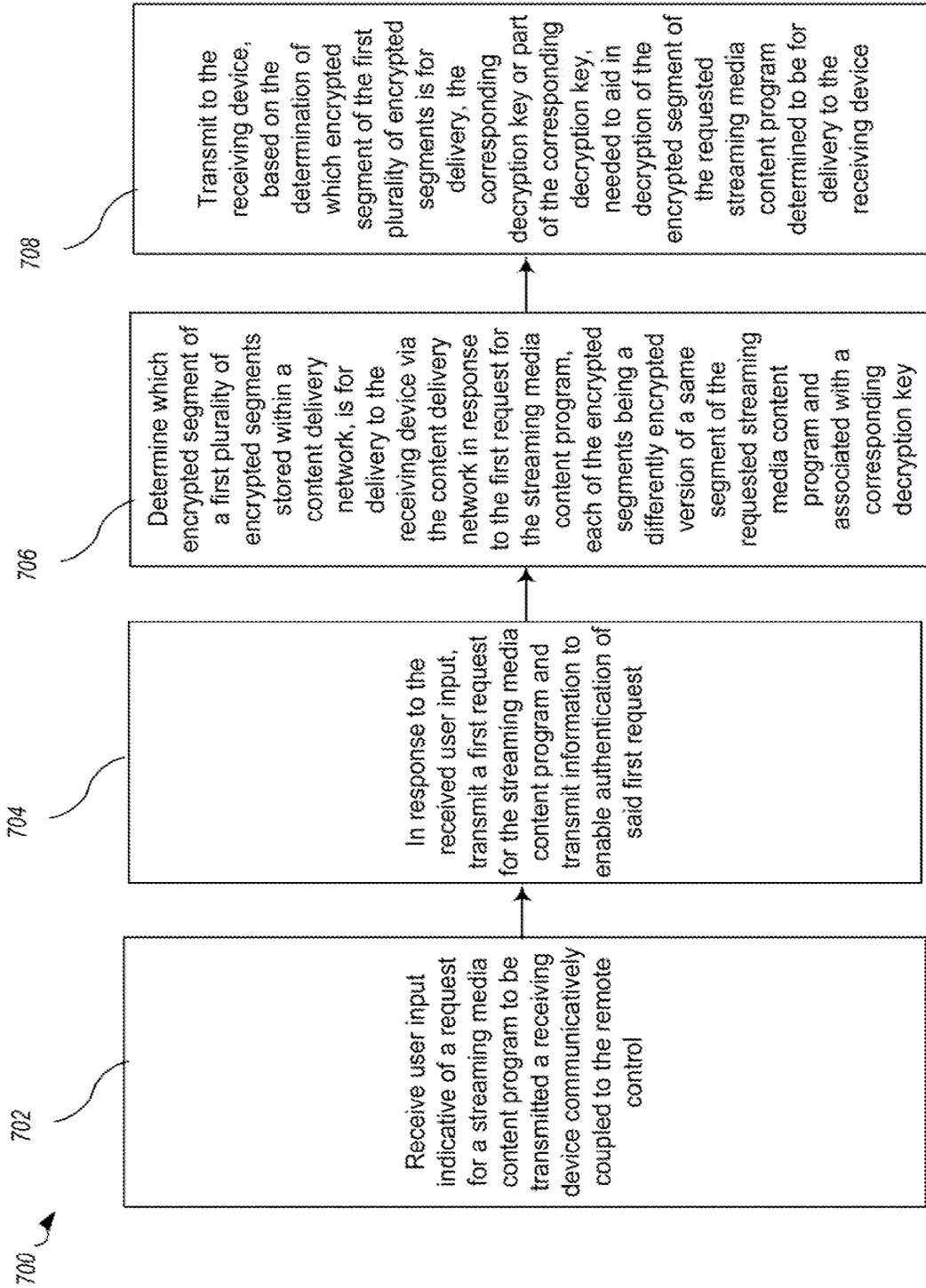


Fig. 7

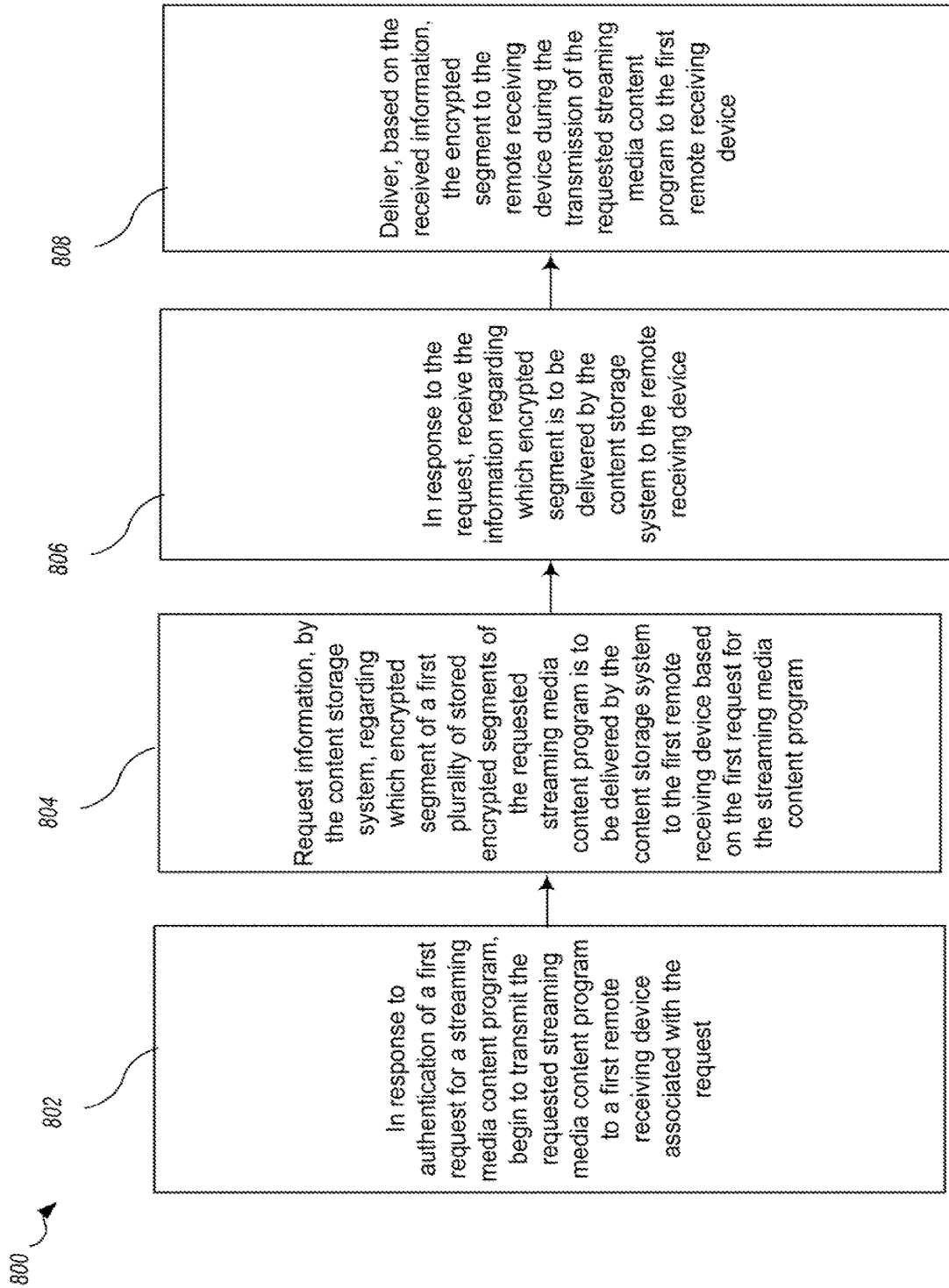


Fig. 8

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/018263

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	<p>PANTOS R ET AL: "HTTP Live Streaming; draft-pantos-http-live-streaming-10.txt", HTTP LIVE STREAMING; DRAFT-PANTOS-HTTP-LIVE-STREAMING-10.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, SWITZERLAND, 15 October 2012 (2012-10-15), pages 1-37, XP015087913, [retrieved on 2012-10-15] pages 20,23,30</p> <p style="text-align: center;">-----</p>	3,6-8,13
X	<p>Frank Hartung ET AL: "DRM Protected Dynamic Adaptive HTTP Streaming", 23 February 2011 (2011-02-23), XP055064987, MMSys'11, February 23-25, 2011, San Jose, California, USA. Retrieved from the Internet: URL:http://www.hartung.fh-aachen.de/publications/ACM_MMSys2011_p277.pdf [retrieved on 2013-06-03]</p>	1,2,4,5,9-12,14,15
Y	<p>the whole document</p> <p style="text-align: center;">-----</p>	3,6-8,13
Y	<p>ANONYMOUS: "Text of ISO/IEC CD 23009-4 Format independent segment encryption and authentication", 100. MPEG MEETING;30-4-2012 - 4-5-2012; GENEVA; (MOTION PICTURE EXPERT GROUP OR ISO/IEC JTC1/SC29/WG11),, no. N12689, 14 May 2012 (2012-05-14), XP030019163, pages 5-9,13</p> <p style="text-align: center;">-----</p>	3,6-8,13

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/018263

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011246616 A1	06-10-2011	US 2011246616 A1 WO 2011123797 A1	06-10-2011 06-10-2011

US 2011231660 A1	22-09-2011	TW 201204011 A US 2011231660 A1 WO 2011119554 A1	16-01-2012 22-09-2011 29-09-2011

Form PCT/ISA/210 (patent family annex) (April 2005)

Electronic Acknowledgement Receipt

EFS ID:	47331974
Application Number:	17943956
International Application Number:	
Confirmation Number:	2316
Title of Invention:	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE
First Named Inventor/Applicant Name:	Alexander Dizengof
Customer Number:	46019
Filer:	Cory Smith/Lisa Mansur
Filer Authorized By:	Cory Smith
Attorney Docket Number:	3010043.2
Receipt Date:	06-JAN-2023
Filing Date:	13-SEP-2022
Time Stamp:	18:01:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	3010043-000002-IDS-Transmittal-Letter.pdf	97093 <small>edf044a8b3f338183563410cea99773bfa0272b</small>	no	1

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	3010043-000002-IDS-Form.pdf	1034647	no	4
			2b3cde688d80f592a433a754bfc0292e736304ee		
Warnings:					
Information:					
3	Foreign Reference	WO-2014158562A1.pdf	524547	no	56
			5a5826c499b93b702b36b56f8d61a92f41028909		
Warnings:					
Information:					
4	Non Patent Literature	NPL-1.pdf	3422640	no	4
			31b481734946e29b1fe53673c6782a17360f8ad		
Warnings:					
Information:					
5	Non Patent Literature	NPL-2.pdf	2261885	no	3
			d06c3dd4589600b080afd0f0fbccf4c58b6b73		
Warnings:					
Information:					
6	Non Patent Literature	NPL-3.pdf	247553	no	2
			f3fade2e5da56ab335d4cb87ebf48a816078b144		
Warnings:					
Information:					
7	Non Patent Literature	NPL-4.pdf	73799	no	1
			d697886fa35024925fd8f6d79d0cc64b695049c		
Warnings:					
Information:					
8	Non Patent Literature	NPL-5.pdf	196403	no	1
			3f8bb277dfd1dc4f8367782e26ecc4afd1fd52		
Warnings:					
Information:					

9	Non Patent Literature	NPL-6.pdf	312371 adad244f00222e371af82be1961f7bc442461d85	no	1
Warnings:					
Information:					
Total Files Size (in bytes):				8170938	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 17/943,956	Filed: September 13, 2022
Applicant: Carbyne Ltd.	Examiner: Lafontant, Gary
Inventor(s): Alexander Dizengof	Art Unit: 2646
Title: System, Method, and Computer-Readable Medium for Streaming Real-Time Data from a User Device	Confirmation No.: 2316

INFORMATION DISCLOSURE STATEMENT

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

Dear Examiner Lafontant:

Applicant requests that the documents identified on the Form PTO/SB/08a enclosed herewith be considered by the Examiner and made of record in this file. The Examiner is also asked to initial copies of the enclosed Form PTO/SB/08a to evidence such consideration.

The filing of this Information Disclosure Statement is not to be construed as an admission that the information cited in the statement is, or is considered to be, material to the patentability of the invention claimed in the above-identified application, or that it qualifies as prior art against any or all of the current claims. Further, no representation is made that a search has been performed.

This Information Disclosure Statement is being filed following the mailing of a first Office Action on the merits but prior to the mailing date of any of: (a) a final action under § 1.113; (b) a notice of allowance under § 1.311; or (c) an action that otherwise closes prosecution in the application. Each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement. Accordingly, no fee is required, and we request the Patent Office to consider the references cited herein. 37 C.F.R. §§1.97(c)-(e). The Commissioner for Patents, however, is hereby authorized to charge any additional fees necessitated by the filing of this paper, or credit any overpayment, to Account No. 02-4467.

Respectfully submitted,

BRYAN CAVE LEIGHTON PAISNER LLP
Two North Central Avenue
Suite 2100
Phoenix, AZ 85004-4406

/Cory G. Smith/
Cory G. Smith
Attorney for Applicant
Reg. No. 63,218
Tel. (602) 364-7442



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 4 columns: APPLICATION NUMBER (17/943,956), FILING OR 371(C) DATE (09/13/2022), FIRST NAMED APPLICANT (Alexander Dizengof), ATTY. DOCKET NO./TITLE (3010043.2)

CONFIRMATION NO. 2316

46019
BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX)
TWO NORTH CENTRAL AVENUE, SUITE 2100
PHOENIX, AZ 85004

PUBLICATION NOTICE



Title:SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE

Publication No.US-2023-0006854-A1

Publication Date:01/05/2023

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	9420116		2016-08-16	Hamilton et al.		
	2	9167379		2015-10-20	Hamilton et al.		
	3	8976939		2015-03-10	Hamilton et al.		
	4	8270935		2012-09-18	Lee		
	5	8145183		2012-03-27	Barbeau et al.		
	6	7751826		2010-07-06	Gardner et al.		
If you wish to add additional U.S. Patent citation information please click the Add button.							Add
U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

1	20140007158		2014-01-02	Bhagwat
2	20120202447		2012-08-09	Edge et al.
3	20120190384		2012-07-26	Marr et al.
4	20120149324		2012-06-14	Daly
5	20120027189		2012-02-02	Shaffer et al.
6	20110111726		2011-05-12	Kholaif et al.
7	20110086607		2011-04-14	Wang et al.
8	20100261492		2010-10-14	Salafia et al.
9	20100220840		2010-09-02	Ray et al.
10	20100174560		2010-07-08	Quan et al.
11	20050176441		2005-08-11	Jurecka

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button.

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	PCT International Search Report and Written Opinion issued in corresponding PCT Application No. PCT/JS2014/051952, mailed November 24, 2014.	

If you wish to add additional non-patent literature document citation information please click the Add button.

EXAMINER SIGNATURE

Examiner Signature	<input type="text"/>	Date Considered	<input type="text"/>
--------------------	----------------------	-----------------	----------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Cory Smith/	Date (YYYY-MM-DD)	2022-12-13
Name/Print	Cory Smith	Registration Number	63218

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour 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. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 58377-433803	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2014/051952	International filing date (<i>day/month/year</i>) 20 August 2014	(Earliest) Priority Date (<i>day/month/year</i>) 21 August 2013
Applicant TRITECH SOFTWARE SYSTEMS		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the language, the international search was carried out on the basis of:

the international application in the language in which it was filed.

a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. This international search report has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2. Certain claims were found unsearchable (see Box No. II).

3. Unity of invention is lacking (see Box No. III).

4. With regard to the title,

the text is approved as submitted by the applicant.

the text has been established by this Authority to read as follows:

5. With regard to the abstract,

the text is approved as submitted by the applicant.

the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

a. the figure of the drawings to be published with the abstract is Figure No. 1

as suggested by the applicant.

as selected by this Authority, because the applicant failed to suggest a figure.

as selected by this Authority, because this figure better characterizes the invention.

b. none of the figures is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/051952

<p>A. CLASSIFICATION OF SUBJECT MATTER IPC(8) - H04W 4/22 (2014.01) CPC - H04M 3/5116 (2014.09) According to International Patent Classification (IPC) or to both national classification and IPC</p>																							
<p>B. FIELDS SEARCHED</p> <p>Minimum documentation searched (classification system followed by classification symbols) IPC(8) - H04W 4/12, H04W 4/14, H04W 4/22 (2014.01) USPC - 379/37, 45; 455/404.1, 466, 521</p> <p>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched CPC - H04M 3/5116; H04W 4/12, H04W 4/14, H04W 4/22, H04W 76/007 (2014.09) (keyword delimited)</p> <p>Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) Orbit, Google Patents, Google. Search terms used: mobile, pda, emergency, 911, call center, PSAP, text, SMS, GUI, user interface, display, url, web, location, GPS</p>																							
<p>C. DOCUMENTS CONSIDERED TO BE RELEVANT</p> <table border="1"> <thead> <tr> <th>Category*</th> <th>Citation of document, with indication, where appropriate, of the relevant passages</th> <th>Relevant to claim No.</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>US 2010/0261492 A1 (SALAFIA et al) 14 October 2010 (14.10.2010) entire document</td> <td>1-7, 9-17, 19-21</td> </tr> <tr> <td>Y</td> <td></td> <td>8, 18, 22 and 23</td> </tr> <tr> <td>Y</td> <td>US 2012/0202447 A1 (EDGE et al) 09 August 2012 (09.08.2012) entire document</td> <td>8, 18, 22 and 23</td> </tr> <tr> <td>A</td> <td>US 2012/0027189 A1 (SHAFFER et al) 02 February 2012 (02.02.2012) entire document</td> <td>1-23</td> </tr> <tr> <td>A</td> <td>US 2011/0086607 A1 (WANG et al) 14 April 2011 (14.04.2011) entire document</td> <td>1-23</td> </tr> <tr> <td>A</td> <td>US 2010/0174560 A1 (QUAN et al) 08 July 2010 (08.07.2010) entire document</td> <td>1-23</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X	US 2010/0261492 A1 (SALAFIA et al) 14 October 2010 (14.10.2010) entire document	1-7, 9-17, 19-21	Y		8, 18, 22 and 23	Y	US 2012/0202447 A1 (EDGE et al) 09 August 2012 (09.08.2012) entire document	8, 18, 22 and 23	A	US 2012/0027189 A1 (SHAFFER et al) 02 February 2012 (02.02.2012) entire document	1-23	A	US 2011/0086607 A1 (WANG et al) 14 April 2011 (14.04.2011) entire document	1-23	A	US 2010/0174560 A1 (QUAN et al) 08 July 2010 (08.07.2010) entire document	1-23
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.																					
X	US 2010/0261492 A1 (SALAFIA et al) 14 October 2010 (14.10.2010) entire document	1-7, 9-17, 19-21																					
Y		8, 18, 22 and 23																					
Y	US 2012/0202447 A1 (EDGE et al) 09 August 2012 (09.08.2012) entire document	8, 18, 22 and 23																					
A	US 2012/0027189 A1 (SHAFFER et al) 02 February 2012 (02.02.2012) entire document	1-23																					
A	US 2011/0086607 A1 (WANG et al) 14 April 2011 (14.04.2011) entire document	1-23																					
A	US 2010/0174560 A1 (QUAN et al) 08 July 2010 (08.07.2010) entire document	1-23																					
<p><input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/></p>																							
<p>* Special categories of cited documents:</p> <table border="0"> <tr> <td> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> </td> <td> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p> </td> </tr> </table>			<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p>																			
<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p>																						
<p>Date of the actual completion of the international search 27 October 2014</p>		<p>Date of mailing of the international search report 24 NOV 2014</p>																					
<p>Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201</p>		<p>Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774</p>																					

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To: D. BENJAMIN ESPLIN
PILLSBURY WINTHROP SHAW PITTMAN LLP
ATTENTION: DOCKETING DEPARTMENT
P.O. BOX 10500
MCLEAN, VA 22102

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing **24 NOV 2014**
(day/month/year)

Applicant's or agent's file reference 58377-433803		FOR FURTHER ACTION See paragraph 2 below	
International application No. PCT/US2014/051952	International filing date (day/month/year) 20 August 2014	Priority date (day/month/year) 21 August 2013	
International Patent Classification (IPC) or both national classification and IPC IPC(8) - H04W 4/22 (2014.01) CPC - H04M 3/5116 (2014.09)			
Applicant TRITECH SOFTWARE SYSTEMS			

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1 bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Date of completion of this opinion 27 October 2014	Authorized officer: Blaine R. Copenheaver PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774
---	--	--

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US2014/051952

Box No. I Basis of this opinion

1. With regard to the language, this opinion has been established on the basis of:
- the international application in the language in which it was filed.
- a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).
2. This opinion has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:
- a. (means)
- on paper
- in electronic form
- b. (time)
- in the international application as filed
- together with the international application in electronic form
- subsequently to this Authority for the purposes of search
4. In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US2014/051952

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	<u>8, 18, 22 and 23</u>	YES
	Claims	<u>1-7, 9-17 and 19-21</u>	NO
Inventive step (IS)	Claims	<u>None</u>	YES
	Claims	<u>1-23</u>	NO
Industrial applicability (IA)	Claims	<u>1-23</u>	YES
	Claims	<u>None</u>	NO

2. Citations and explanations:

Claims 1-7, 9-17 and 19-21 lack novelty under PCT Article 33(2) as being anticipated by Salafia et al (hereinafter referred to as Salafia).

Regarding claim 1, Salafia disclose a system configured to provide, to emergency operators, communication through textual messages, (providing emergency operators [call handlers within a public safety answering point (PSAP)] the ability to communicate using textual messages, para. 0062-0063), the system comprising: one or more processors configured to execute computer program modules, (a processor for executing program modules such as call handling, para. 0010 and 0020-0021), the computer program modules comprising: a call reception module configured to receive incoming emergency voice calls being placed to an emergency call center through an emergency communications network from wireless mobile devices, the incoming emergency voice calls including a first voice call placed from a first wireless mobile device; (an emergency call center [PSAP] receiving an incoming emergency voice call through cellular and PSTN networks from a wireless mobile device [cell phone], para. 0064-0066), an outgoing message module configured to generate outgoing textual messages for transmission to wireless mobile devices from which incoming emergency voice calls are received such that a first outgoing textual message is generated for transmission to the first wireless mobile device based on the first voice call; (the PSAP call handler generating an outgoing textual message for transmission to the cell phone from which the incoming emergency voice call was received, para. 0069-0071), and a transmission module configured to transmit the outgoing textual messages to the appropriate wireless mobile devices through a second communications network that is different than the emergency communications network such that the first outgoing textual message is transmitted to the first wireless mobile device through the second communications network, (the PSAP call handler transmitting the outgoing textual message to the cell phone through an Internet network that is different than the previously used networks , para. 0072-0073).

Regarding claim 11, Salafia disclose a computer-implemented method for providing, to emergency operators, communication through textual messages, (providing emergency operators [call handlers within a PSAP] the ability to communicate using textual messages, para. 0062-0063), the method being performed by one or more processors configured to execute computer program modules, (a processor for executing program modules such as call handling, para. 0010 and 0020-0021), the method comprising: receiving incoming emergency voice calls being placed to an emergency call center through an emergency communications network from wireless mobile devices, the incoming emergency voice calls including a first voice call from a first wireless mobile device; (an emergency call center [PSAP] receiving an incoming emergency voice call through cellular and PSTN networks from a wireless mobile device [cell phone], para. 0064-0066), generating outgoing textual messages for transmission to wireless mobile devices from which incoming emergency voice calls are received such that a first outgoing textual message is generated for transmission to the first wireless mobile device based on the first voice call; (the PSAP call handler generating an outgoing textual message for transmission to the cell phone from which the incoming emergency voice call was received, para. 0069-0071), and transmitting the outgoing textual messages to the appropriate wireless mobile devices through a second communications network that is different than the emergency communications network such that the first outgoing textual message is transmitted to the first wireless mobile device through the second communications network, (the PSAP call handler transmitting the outgoing textual message to the cell phone through an Internet network that is different than the previously used networks , para. 0072-0073).

Regarding claims 2 and 12, Salafia further disclose a presentation module configured to present incoming emergency voice calls to emergency operators through a user interface, (a terminal presenting a visual display of incoming emergency voice call data to call handlers, para. 0066), wherein the user interface includes a set of user-selectable options, (the PSAP call handler selects from options (forms, a button, or templates) on the display, para. 0068-0069), and wherein the presentation module is further configured to receive user input from emergency operators to select one or more of the set of user-selectable options, (the display receives a selection from the call handler to selects from one of the options on the display, para. 0070).

Regarding claims 3 and 13, Salafia further disclose wherein the set of user-selectable options correspond to different informational requests associated with the incoming emergency calls such that the first voice call is associated with a first informational request, (the PSAP call handler may request different information associated with the emergency voice call such as request for caller location and images relating to the emergency, para. 0069), and wherein the first informational request is included in the first outgoing textual message, (the request is included in the outgoing textual message, para. 0070).

Regarding claims 4 and 14, Salafia further disclose wherein the first informational request includes emergency instructions, (the request for information includes emergency instructions, para. 0023-0024 and 0072-0073).

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US2014/051952

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

Regarding claims 5 and 15, Salafia further disclose wherein the first outgoing textual message includes a link to emergency instructions, (the outgoing textual message includes a link [Uniform Resource Locators (URLs)] to instructions on how to handle a situation, para. 0010-0011 and 0120).

Regarding claims 6 and 16, Salafia further disclose wherein the outgoing textual messages include one or both of short message service (SMS) messages and/or multimedia messaging service (MMS) messages, (the outgoing textual messages include MMS messages, para. 0008 and 0130).

Regarding claims 7 and 17, Salafia further disclose a web-hosting module configured to host web resources configured to: (i) query wireless mobile devices for location information, (requesting location information from the cell phone over an Internet network, para. 0056, 0069 and 0073), and (ii) share, responsive to receipt of location information, received location information with the presentation module, (the received location information is displayed to the PSAP call handler, para. 0066 and 0076-0077), wherein the first outgoing textual message includes a uniform resource locator (URL) link to the web resources, (the outgoing textual message includes a URL [a web address which links to web resources], para. 0011 and 0119-0120), wherein the presentation module is further configured to present shared queried location information to emergency operators through the user interface, (the PSAP call handlers view the displayed location information via the user interface [workstation terminal], para. 0061 and 0066).

Regarding claims 9 and 19, Salafia further disclose wherein the transmission module is further configured to receive textual messages from wireless mobile devices through the second communications network, (the cell phone transmits textual messages to the PSAP via the Internet, the second network, para. 0062).

Regarding claims 10 and 20, Salafia further disclose wherein the presentation module is further configured to present received textual messages through the user interface, (textual messages are displayed via the user interface [workstation terminal], para. 0066 and 0077).

Regarding claim 21, Salafia disclose a computer-implemented method for providing, to emergency operators, communication through textual messages, (providing emergency operators [call handlers within a public safety answering point (PSAP)] the ability to communicate using textual messages, para. 0062-0063), the method being performed by one or more processors configured to execute computer program modules, (a processor for executing program modules such as call handling, para. 0010 and 0020-0021), the method comprising: receiving incoming emergency voice calls being placed to an emergency call center through an emergency communications network from wireless mobile devices, the incoming emergency voice calls including a first voice call from a first wireless mobile device; (an emergency call center [PSAP] receiving an incoming emergency voice call through cellular and PSTN networks from a wireless mobile device [cell phone], para. 0064-0066), generating outgoing textual messages for transmission to wireless mobile devices from which incoming emergency voice calls are received such that a first outgoing textual message is generated for transmission to the first wireless mobile device based on the first voice call, (the PSAP call handler generating an outgoing textual message for transmission to the cell phone from which the incoming emergency voice call was received, para. 0069-0071), wherein the first outgoing textual message includes textual emergency instructions; (the outgoing textual message includes emergency instructions, para. 0023-0024, 0029 and 0072-0073), and transmitting the outgoing textual messages to the appropriate wireless mobile devices such that the first outgoing textual message is transmitted to the first wireless mobile device, (the PSAP call handler transmitting the outgoing textual message to the cell phone that originated the emergency call, para. 0072-0073).

Claims 8, 18, 22 and 23 lack an inventive step under PCT Article 33(3) as being obvious over Salafia in view of Edge et al (hereinafter referred to as Edge).

Regarding claims 8 and 18, Salafia disclose the invention above but does not specifically disclose the web resources is configured to query wireless mobile devices for location information through an application programming interface (API) function that accesses one or both of global positioning system (GPS) information and/or geolocation information.

Edge is in the field of supporting location privacy via provisioning of a location Uniform Resource Identifier (URI) (para. 0003) and teach wherein the web resources is configured to query wireless mobile devices for location information through an application programming interface (API) function that accesses one or both of global positioning system (GPS) information and/or geolocation information, (querying a cell phone for its location information using an API [a Secure User Plane Location (SUPL) used by a Location Platform (SLP)] to access GPS information, para. 0028 and 0039). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the location information as taught in Edge with the invention of Salafia in order to improve the handling of location privacy. (see Edge, para. 0029).

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2014/051952

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of:

Regarding claim 22, Salafia disclose a computer-implemented method for providing, to emergency operators, communication through textual messages, (providing emergency operators [call handlers within a public safety answering point (PSAP)] the ability to communicate using textual messages, para. 0062-0063), the method being performed by one or more processors configured to execute computer program modules, (a processor for executing program modules such as call handling, para. 0010 and 0020-0021), the method comprising: receiving incoming emergency voice calls being placed to an emergency call center through an emergency communications network from wireless mobile devices, the incoming emergency voice calls including a first voice call from a first wireless mobile device; (an emergency call center [PSAP] receiving an incoming emergency voice call through cellular and PSTN networks from a wireless mobile device [cell phone], para. 0064-0066), generating outgoing textual messages for transmission to wireless mobile devices from which incoming emergency voice calls are received such that a first outgoing textual message is generated for transmission to the first wireless mobile device based on the first voice call, (the PSAP call handler generating an outgoing textual message for transmission to the cell phone from which the incoming emergency voice call was received, para. 0069-0071), wherein the first outgoing textual message includes a uniform resource locator (URL) link to a web-hosted application, (the outgoing textual message includes a URL [a web address which links to web resources], para. 0011 and 0118-0120), transmitting the outgoing textual messages to the appropriate wireless mobile devices such that the first outgoing textual message is transmitted to the first wireless mobile device; (the PSAP call handler transmitting the outgoing textual message to the cell phone that originated the emergency call, para. 0072-0073).

Salafia disclose the invention above but does not specifically disclose querying the first wireless mobile device for location information and obtaining, responsive to the first wireless mobile device being queried, the location information. However, Edge teach a (URL) link to a web hosted application configured to query the first wireless mobile device for location information, (a URI [a common form of URL] link to an application configured to query the mobile device [SET] for location information 220, Fig. 2A, para. 0039 and 0049-0050), and obtaining, responsive to the first wireless mobile device being queried, the location information, (obtaining the location information 230 from the queried SET, para. 0050). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the location information as taught in Edge with the invention of Salafia in order to improve the handling of location privacy. (see Edge, para. 0029).

Regarding claim 23, Salafia disclose a computer-implemented method for providing location information to emergency operators, (providing location information to emergency operators [call handlers], para. 0005), the method being performed by one or more processors configured to execute computer program modules, (a processor for executing program modules such as call handling, para. 0010 and 0020-0021), the method comprising: hosting web resources that is accessible through a uniform resource locator (URL) address; (the PSAP includes an incident linked multimedia system [ILMS] which has web hosting capabilities accessible through a URL address, para. 0118-0120 and 0127), receiving a request from a wireless mobile device; (receiving a request for emergency services from a wireless device [cell phone], para. 0065-0066), receiving an identifier associated with the request; (receiving an identifier [telephone number of the caller] associated with the request, para. 0066), transmitting a response to the wireless mobile device, (the PSAP call handler transmitting a response to the cell phone caller, para. 0073), wherein the response includes a query for location information, (requesting location information from the cell phone, para. 0056 and 0069).

Salafia disclose the invention above but does not specifically disclose receiving, from the wireless mobile device, the queried location information and providing the queried location information and the received identifier to one or more emergency operators. However, Edge teach receiving, from the wireless mobile device, the queried location information, (receiving from the mobile device [SET] queried location information 220, Fig. 2A and para. 0039 and 0049-0050), and providing the queried location information and the received identifier to one or more emergency operators, (providing the queried location information and the received identifier [URI] to emergency operators [external client], para. 0049-0050 and 0079). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the location information as taught in Edge with the invention of Salafia in order to improve the handling of location privacy. (see Edge, para. 0029).

Claims 1-23 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.

Electronic Acknowledgement Receipt

EFS ID:	47198526
Application Number:	17943956
International Application Number:	
Confirmation Number:	2316
Title of Invention:	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE
First Named Inventor/Applicant Name:	Alexander Dizengof
Customer Number:	46019
Filer:	Cory Smith/Lisa Mansur
Filer Authorized By:	Cory Smith
Attorney Docket Number:	3010043.2
Receipt Date:	13-DEC-2022
Filing Date:	13-SEP-2022
Time Stamp:	17:15:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	3010043-000002-IDS-Transmittal-Letter.pdf	95931 <small>1016bd074c2715b4d05c2778859567cd17174df</small>	no	1

Warnings:

Information:					
2	Information Disclosure Statement (IDS) Form (SB08)	3010043-000002-IDS-1.pdf	1042193	no	5
			b05228028d96d2d6d958c23a005f857c30260d65		
Warnings:					
Information:					
3	Foreign Reference	EP-2992692.pdf	5032715	no	75
			aa7a1ed80bc5d768b094324f9989b932d72cd358		
Warnings:					
Information:					
4	Non Patent Literature	1-NPL-1.pdf	57354	no	2
			e1da7029763c298ed439123aab32bd33b2e4f1a6		
Warnings:					
Information:					
5	Non Patent Literature	1-NPL-2.pdf	61902	no	2
			fc3a73cf973b3d50e553a784c0d87d07ef6c1cb5		
Warnings:					
Information:					
6	Information Disclosure Statement (IDS) Form (SB08)	3010043-000002-IDS-2.pdf	1034662	no	5
			5d581eef6edef8d1ef7f425d24fbb02612809a4d		
Warnings:					
Information:					
7	Non Patent Literature	2-NPL-1.pdf	435673	no	7
			9163d595f5f68330c6dc4eb06755c2ce4bbad433		
Warnings:					
Information:					
Total Files Size (in bytes):				7760430	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 17/943,956	Filed: September 13, 2022
Applicant: Carbyne Ltd.	Examiner: Lafontant, Gary
Inventor(s): Alexander Dizengof	Art Unit: 2646
Title: System, Method, and Computer-Readable Medium for Streaming Real-Time Data from a User Device	Confirmation No.: 2316

INFORMATION DISCLOSURE STATEMENT

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

Dear Examiner Lafontant:

Applicant requests that the documents identified on the (2) Forms PTO/SB/08a enclosed herewith be considered by the Examiner and made of record in this file. The Examiner is also asked to initial copies of the enclosed Forms PTO/SB/08a to evidence such consideration.

The filing of this Information Disclosure Statement is not to be construed as an admission that the information cited in the statement is, or is considered to be, material to the patentability of the invention claimed in the above-identified application, or that it qualifies as prior art against any or all of the current claims. Further, no representation is made that a search has been performed.

This Information Disclosure Statement is being filed (1) within three months of the filing date of a national application other than a continued prosecution application, (2) within three months of the date of entry of the national stage, (3) before the mailing of a first Office Action on the merits, or (4) before the mailing of a first Office Action after the filing of a request for continued examination. Accordingly, no fee is required. The Commissioner for Patents, however, is hereby authorized to charge any additional fees necessitated by the filing of this paper, or credit any overpayment, to Account No. 02-4467.

Respectfully submitted,

BRYAN CAVE LEIGHTON PAISNER LLP
Two North Central Avenue
Suite 2100
Phoenix, AZ 85004-4406

/Cory G. Smith/
Cory G. Smith
Attorney for Applicant
Reg. No. 63,218
Tel. (602) 364-7442

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	10686618		2020-06-16	Dizengof		
	2	9792654		2017-10-17	Limas et al.		
	3	9414225		2016-08-09	Timariu et al.		
	4	9301117		2016-03-29	Leggett et al.		
	5	8504090		2013-08-06	Klein et al.		
If you wish to add additional U.S. Patent citation information please click the Add button.							Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	20200313922		2020-10-01	Dizengof		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

2	20190052474	2019-02-14	Dizengof
3	20170180964	2017-06-22	Mehta et al.
4	20170164175	2017-06-08	Bozik et al.
5	20170126751	2017-05-04	Stach et al.
6	20170124853	2017-05-04	Mehta et al.
7	20160381091	2016-12-29	O'Connor et al.
8	20160088455	2016-03-24	Bozik et al.
9	20160014585	2016-01-14	Sundararaj et al.
10	20150099482	2015-04-09	Schmitz
11	20150056946	2015-02-26	Leggett et al.
12	20070028279	2007-02-01	Kim

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ^{2]}	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2992692	EU		2016-03-09	Decharms		

If you wish to add additional Foreign Patent Document citation information please click the Add button.

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	European Search Report and the European Search Opinion Dated 08 April 2022 from the European Patent Office Re. Application No. 22152510.8, (11 Pages).	
	2	European Search Report and the European Search Opinion Dated 06 December 2018 from the European Patent Office Re. Application No. 18188748.0, (10 Pages).	

If you wish to add additional non-patent literature document citation information please click the Add button.

EXAMINER SIGNATURE

Examiner Signature	<input type="text"/>	Date Considered	<input type="text"/>
--------------------	----------------------	-----------------	----------------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	17943956
	Filing Date	2022-09-13
	First Named Inventor	Alexander Dizengof
	Art Unit	2646
	Examiner Name	Lafontant, Gary
	Attorney Docket Number	3010043.2

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Cory Smith/	Date (YYYY-MM-DD)	2022-12-13
Name/Print	Cory Smith	Registration Number	63218

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour 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. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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.



(11) **EP 2 992 692 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
29.08.2018 Bulletin 2018/35

(21) Application number: **14794088.6**

(22) Date of filing: **05.05.2014**

(51) Int Cl.:
H04W 4/021 ^(2018.01) **H04W 76/14** ^(2018.01)
H04W 4/90 ^(2018.01) **H04N 7/14** ^(2006.01)
H04L 29/08 ^(2006.01) **H04N 7/15** ^(2006.01)
H04W 4/02 ^(2018.01) **H04M 3/56** ^(2006.01)
H04L 29/06 ^(2006.01) **G06Q 50/26** ^(2012.01)
H04M 1/1725 ^(2006.01)

(86) International application number:
PCT/US2014/036871

(87) International publication number:
WO 2014/182638 (13.11.2014 Gazette 2014/46)

(54) **MOBILE SECURITY TECHNOLOGY**
MOBILE SICHERHEITSTECHNOLOGIE
TECHNOLOGIE DE SÉCURITÉ MOBILE

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **04.05.2013 US 201361819575 P**
31.08.2013 US 201361872690 P
08.01.2014 US 201461924901 P

(43) Date of publication of application:
09.03.2016 Bulletin 2016/10

(73) Proprietor: **DECHARMS, Christopher**
Montara, CA 94037 (US)

(72) Inventor: **DECHARMS, Christopher**
Montara, CA 94037 (US)

(74) Representative: **Granleese, Rhian Jane**
Marks & Clerk LLP
90 Long Acre
London WC2E 9RA (GB)

(56) References cited:
US-A1- 2008 267 360 US-A1- 2011 111 728
US-A1- 2011 117 878 US-A1- 2012 087 212
US-A1- 2012 310 956 US-A1- 2013 040 600
US-A1- 2013 040 600

EP 2 992 692 B1

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Description

Summary

Cross-Reference to Related Applications

[0001] This application claims priority to U.S. Provisional Application Serial No. 61/819,575, which is entitled "Mobile Security Technology" and was filed on May 4, 2013; to U.S. Provisional Application Serial No. 61/872,690, which is entitled "Mobile Security Technology" and was filed on August 31, 2013; and to U.S. Provisional Application Serial No. 61/924,901, which is entitled "Mobile Security Technology" and was filed on January 8, 2014.

Technical Field

[0002] This document generally describes computer-based technologies related to security. For example, this document describes, among other things, mobile computing devices that provide security features through the use of a variety of computer-based technologies, such as one-way, two-way, or multi-party video chat and/or video conferencing technology.

Background

[0003] Computer-based technologies have been used for security and video surveillance. For example, computer-based technology has been developed allow for users to stream live video feeds from security cameras over the internet and on remote computing devices, such as laptop computers, desktop computers, and mobile computing devices.

[0004] US2011/0111728 A1 discloses a system and method for providing a conduit to send information to emergency services from a wireless device. Systems and methods for registering an alarm button on a wireless device and sending to public and/or private emergency services providers information related to the wireless device including its location, information about a wireless device end user and/or subscriber associated with the wireless device, and information recorded by one or more wireless devices during and subsequent to the time the alarm button is activated.

[0005] US2013/0040600 A1 discloses a notification and tracking system for a mobile device. The system includes a mobile device application that is adapted to be stored in memory on the mobile device. The application, upon activation, determines the GPS coordinates of the mobile device, records digital images over a period of time, sends a preset message from the mobile device to at least one recipient, preferably an emergency responder, such as a security monitoring station, and sends the GPS coordinates and the digital images. The coordinates and images may be sent to a remote server for storage and which can be accessed by the emergency responder. The coordinates and images are periodically updated and sent while the program is activated.

[0006] This document generally describes computer-based technologies to provide security and assistance to users whenever they are in need of such services, such as when users are in dangerous or uncertain physical situations in which their safety or the safety of others may be in jeopardy. For example, the disclosed technologies can allow for users to quickly obtain access to and to involve appropriate remote parties in their current physical situation in an effort to avoid any harm from befalling the users, while at the same time storing information (e.g., video recording) regarding the incident at a secure and remote storage facility. Such access and involvement of remote parties can be provided through the use of any of a variety of appropriate techniques, such as two-way remote monitoring, remote imaging, audio and video conferencing and remote control technology on mobile computing devices, such as cell phones, smartphones, personal digital assistants (PDAs), tablets, wearable computing devices (e.g., GOOGLE GLASS, Looxcie, GoPro), and/or other devices that can provide connection between users and increase users security. For example, a user may initiate two-way video conferencing with a friend, police, or emergency responder as a means of allowing the responder to help facilitate a secure outcome for the user.

[0007] The invention is defined by a method according to claim 1 and a device according to claim 9. Further embodiments are defined in the dependent claims.

[0008] Implementations of the disclosed technology can be methods that include one or more of the following features: two-way audiovisual teleconferencing between two computing devices over a network connection (A); transmitting and receiving, by an application running on a mobile computing device, real-time audio and video with another computing device over a network connection (B); communicating, by a mobile computing device, with another computing device as part of a two-way video chat session over a network connection; and displaying, as part of the two-way video chat session, real-time video from the other computing device while transmitting real-time video from the mobile computing device to the other computing device (C); the network connection can be a peer-to-peer connection (D); identifying a plurality of candidate responders, and selecting a particular candidate responder based, at least in part, on one or more factors (E); the factors can include one or more of: a user location, a responder location, responder ratings, responder skills and/or training, type of situation, and a predefined list of responders (F); determining a location of a mobile computing device using one or more of a plurality of data sources (G); the data sources can include one or more of: GPS, WiFi, beacon signals, other data transmitted by radiofrequency that is useable to electronically locate a device (H); determining or receiving a geographic location for a user, and identifying, using a database of locations and corresponding responders, one or more appro-

appropriate responders based, at least in part, on said geographic location (I); the database of locations can be a PSAP database (J); receiving a geographic location for a user, and determining, using a database of locations and corresponding licensure status, whether said user is located within one or more licensed jurisdictions (L); the licensed jurisdiction can include an area where an entity has been granted a right to perform a service (M); receiving a request to connect a mobile computing device with a responder service, identifying an appropriate responder service based on the location of the mobile computing device, and initiating contact with the appropriate responder service on behalf of the mobile computing device (N); the request can be one or more of: a text message, a verbal request, selection of call 911 feature, and can be received over peer-to-peer network connection (O); the location can be one or more of a geolocation and real-time location updates (P); initiating contact can include one or more of: establish communication session between mobile device and emergency service, and communication on behalf of the mobile computing device (Q); the responder service can be an emergency dispatch system (R); receiving a message and the location of the mobile computing device of a user, determining an appropriate emergency responder service based on the location, initiating a telephone call to appropriate the emergency responder service on behalf of the user, and transmitting the message to the emergency responder service (S); the message can be sent with one or more of the user's profile and the user's contact information, and can be included with initiating three-way communication with the user (T); receiving a text message requesting emergency responder services for a user of a mobile computing device, the text message identifying a location of the mobile computing device, determining an appropriate emergency responder service based on the location, and initiating a telephone call to appropriate the emergency responder service on behalf of the user (U); receiving a message and the location of the mobile computing device of a user, determining an appropriate responder service based on the location, initiating electronic communication with the appropriate responder service for the user, and transmitting the message to the responder service (V); the electronic communication can include one or more of: communication between the mobile computing device and the emergency responder service, communication between the central system and the emergency responder service, and the electronic communication can include information about the user (W); the responder service can be an emergency dispatch system (X); providing the user's profile, providing the user's contact information, and/or initiating three-way communication with the user (Y); recording video using one or more cameras that are accessible to a computing device, modifying the video by adding one or more features, and transmitting the modified video with the features to a remote storage system for persistent storage (Z); the one or more cameras can include cameras connected to

the computing device and wirelessly connected to the computing device (AA); the features can include one or more of: identifying features, security features, and verification features (AB); the identifying features can include user identification (AC); the security features can include encryption (AD); the verification features can include one or more of: a timestamp, a digital watermark, and location information (AE); recording a video using one or more cameras mounted to a user's body that are accessible to a computing device (AF); receiving data recorded by a computing device during an incident, identifying one or more features from the data, and determining an identity of an assailant involved in the incident based on comparison of the one or more features with information stored in one or more data sources (AG); the data can include one or more of: video data, image data, audio data, and other data detected from wireless devices (AH); the features can include one or more of: face, voice, gate, proportions, and device identity (AI); the data sources can include one or more of: criminal databases, law enforcement data sources, social network data sources, and user data (AJ); the user data can include one or more of contacts, friend lists, and a user's images (AK); recording video using one or more security cameras that are accessible to a mobile computing device, and transmitting the video to a remote storage system for persistent storage (AL); the security cameras can include one or more of remote camera and camera acting in security camera mode (AM); receiving, at a computing device, input to send a push notification to another device, determining a current location of the computing device, and transmitting a push notification to the other device that includes the current location (AN); the other device can be specified by user input or determined based on multifactor input (AO); receiving, at a computing device, input to send a push notification to another device, determining a current location of the other device, determining whether the other device's current location is within a specified distance from a specified location, and if the other device's current location is within a specified distance from a specified location, transmitting a push notification to the other device that includes the current location (AP); receiving, at a computing device, a location of a responder through a network connection, and displaying the location of the responder on the computing device (AQ); the network connection can be received while concurrent video chat going on (AR); displaying the location can include one or more of: the location being displayed on map, icon depicting responder displayed on map, image of responder displayed on map, map presented with video feed, and location presented with regard to location of user device (AS); receiving information determining whether responders are currently available for a user of a computing device, and if no responders are currently available, taking an appropriate action (AT); the appropriate action can include one or more of: presenting a message on the computing device that no responders are available, providing information to user re-

lating to alternate actions, and routing user's request(s) to a backup solution (AU); presenting can include one or more of: visual display, audio output, and haptic feedback (AV); receiving information determining whether responders are currently available for a user of a computing device, and if no responders are currently available, presenting a warning message on the computing device that no responders are available (AW); establishing, before initiating a communication session at a computing device, peer-to-peer network connections with a plurality of other devices associated with candidate responders, and obtaining and displaying, using the network connections, current status information for a plurality of candidate responders (AX); establishing, before initiating a two-way audiovisual communication session at a computing device, peer-to-peer network connections with a plurality of other devices associated with candidate responders, and obtaining and displaying, using the network connections, one-way video depicting a plurality of candidate responders (AY); receiving, at a computing device and from a responder computing device, instructions to perform one or more operations, determining whether the responder computing device is permitted to remotely control operation of the computing device, and performing, based on the determining, the one or more operation (AZ); operations can include one or more of: initiating a communication session with another computing device, initiating an audio communication session with another computing device, initiating a two-way audiovisual communication session with another computing device, initiating a one-way audiovisual communication session with another computing device, activating/deactivating one or more devices (camera, microphone, audio volume, light), recording video, taking a picture, playing an alarm, playing a pre-recorded message, and outputting image/audio/video (BA); displaying a map that depicts geographically associated crime information (BB); displaying a map that depicts geographically associated crime information, receiving new crime information in substantially real time, and updating the map to additionally depict the new crime information (BC); outputting, when the location associated with the new crime information is within a threshold distance from the user's current location, information to the user (BD); transmitting a request to a computer system for a network address of another computing device, receiving, from the computer system, the network address, and establishing, using the network address, a peer-to-peer network connection with the other computing device (BE); receiving input to connect to each member of a group of users, obtaining network addresses for devices associated with the members of the group of users, and sending messages requesting network connections with the devices using the network addresses (BF); the group of users can include one or more of: friends, responders, emergency personnel, and user from designated lists (BG); providing, on a mobile computing device, an interface through which the mobile computing device acts as a user device in personal emer-

gency response system, determining that an input received through the interface is one of a plurality of designated inputs to initiate communication with an emergency response system, and initiating, based on the determining, communication with the emergency response system (BH); recording, by a mobile computing device mounted within a user's home, video by using a camera of the mobile computing device, and transmitting the video to a computer system with additional data obtained by the mobile computing device (BI); the additional data can include location information and user information (BJ); obtaining status information for a one or more users that are associated with one or more computing devices, and outputting the status information (BK); the status information can include an image of the user, a video of the user, whether the user is available, whether the user is on a call, whether the user is away, and whether the user is actively using the device (BL); receiving location information for a user associated with a computing device, determining, using the location information, whether the user has crossed over a boundary of a defined geographic area, and outputting an alert in response to the determining (BM); providing, by a computer system, communication operating across a plurality of different computing platforms and operating systems (BN); the computing platforms and operating systems can include one or more of: iOS, Android, Windows, WindowsMobile, Blackberry, and MacOS (BO); receiving, at a computing device associated with a user and from a responder device, instructions to contact a friend of the user, identifying an appropriate friend to contact, and initiating a communication session with a computing device associated with the identified friend (BP); encrypting, by a computing device, real-time data with associated metadata that identifies when, where, or by whom the real-time data was collected, and transmitting the real-time data (BQ); a central computer system can be a professional emergency response system (BR); gating access to one or more security features based on subscription levels for users (BS); obtaining network addresses for computing devices associated with a user's friends, and automatically initiating network connections with the computing devices (BT); sending and receiving, by a computing device, text messages with other computing devices, and displaying the text messages on the computing device (BU); detecting wireless signals from other nearby devices, and recording and transmitting information regarding the detected wireless signals and the other devices (BV); displaying on a map the locations of users #2 who have begun using an application based on a recommendation from the user in color #1, and displaying on a map the locations of users who have begun using a mobile application based on a recommendation from the users #2 in color #2 (BW); displaying on a map the locations of users who have begun using a mobile application based on a recommendation from the users #3 in color #3 (BX); displaying on a map the locations of users who have begun using a mobile application based on a recommendation

from the users #4 in color #4 (BY); the application can include one or more of: a security application, a social networking application, and an application that was either directly or indirectly provided to the users (BZ); receiving a current location for a user, determining a current safety level for the user at the current location based on one or more factors (CA); the factors can include one or more of: location, crime information, current time, user's profile, user's age, user's gender, available responders, and proximity of responders to the user (CB); a communication protocol that is used can be webRTC (CC); selecting, from among a plurality of responders, one or more responders based, at least in part, on user-generated ratings for the plurality of responders (CD); outputting a graphical user interface element can include a slider through which a user can browse a group of users through linear swiping inputs (CE); receiving a request to transmit a location to another computing device, determining the location of the computing device, and transmitting the location to another computing device (CF); a data source from which user contact information and location information is obtained can be social media (CG); information can be transmitted through a social media platform (CH); receiving input describing an incident, collecting additional details detected or sensed by the mobile computing device regarding the incident, and reporting the incident using the input and the additional details (CI); the additional details can include one or more of: geographic location, images, and video (CJ); information regarding a user can be stored as a user profile (CK); and displaying a video instructing a user how to operate a mobile security application (CL).

[0009] The features A-CL can be combined in any of a variety of appropriate ways. For example, the features A-CL, including all possible subsets thereof, can be used in every possible combination and in every possible permutation.

[0010] Implementations of the disclosed technology can be computing devices and/or computer systems that include one or more of the following features: means to engage in two-way audiovisual teleconferencing with another computing device through a network (CM); means to capture an audio and video datastream #1 (CN); means to transfer said audio and video datastream #1 to another computing device (CO); means to receive audio and video datastream #2 from another computing device (CP); means to display video from said audio and video datastream #2 (CQ); means to present audio from said audio and video datastream #2 (CR); means to receive audio and video from another computing device (CS); a camera, a network interface that is programmed to transmit real-time video recorded by camera to another computing device over a network connection, and to receive real-time video recorded by the other computing device, and a display that is programmed to display, concurrently with transmitting the real-time video, the real-time from the other computing device (CT); a camera, a network interface that is programmed to communicate

with another computing device as part of a two-way video chat session over a network connection, and a display that is programmed to display, as part of the two-way video chat session, real-time video from the other computing device while transmitting real-time video from the mobile computing device to the other computing device (CU); a mobile security application that is programmed to identify a plurality of candidate responders; and select a particular candidate responder based, at least in part, on one or more factors (CV); a geographic location unit that is programmed to determine a location of a mobile computing device using one or more of a plurality of data sources (CW); a network interface that is programmed to receive a geographic location for a user, a database of locations and corresponding responders, and a routing system programmed to identify one or more appropriate responders based, at least in part, on the geographic location for said user and said database (CX); a jurisdiction module that is programmed to determine, for an assistance request for a user, whether the user is located within one or more licensing jurisdictions, and a responder identification module that is programmed to identify a responder to provide assistance to the user based on the determination of whether the user is located within the licensing jurisdictions (CY); a network interface that is programmed to receive a request to connect a mobile computing device with an responder service, an emergency routing system that is programmed to identify an appropriate emergency responder service based on the location of the mobile computing device, and connection manager that is programmed to initiate contact with the appropriate emergency responder service on behalf of the mobile computing device (CZ); a network interface that is programmed to receive a message from a mobile computing device, the message including a location of the mobile computing device, a routing system that is programmed to determine an appropriate responder service based on the location, and connection manager that is programmed to initiate a telephone call to appropriate the emergency responder service on behalf of the user (DA); a network interface that is programmed to receive a message from a mobile computing device, the message including a location of the mobile computing device, a routing system that is programmed to determine an appropriate responder service based on the location, and connection manager that is programmed to initiate electronic communication with the appropriate responder service for the user and transmit the message (DB); one or more cameras that are programmed to record video, a security layer that is configured to modify the video to add one or more features, and a network interface that is configured to transmit the modified video with the features to a remote storage system for persistent storage (DC); one or more cameras mounted to a user's body that are accessible to a computing device (DD); a network interface that is programmed to receive data recorded by a computing device during an incident, a feature identification module that is programmed to

identify one or more features from the data, and an assailant identifier that is programmed to determine an identity of an assailant involved in the incident based on comparison of the one or more features with information stored in one or more data sources (DE); one or more security cameras that are configured to record video on a mobile computing device, and a network interface that is programmed to transmit the video to a remote storage system for persistent storage (DF); a user interface that is programmed to receive input to send a push notification to another device, a location unit that is programmed to determine a current location of the computing device, and a network interface that is programmed to transmit a push notification to the other device that includes the current location (DG); a user interface that is programmed to receive input to send a push notification to another device, a location unit that is programmed to determine a current location of the computing device, and a network interface that is programmed to transmit a push notification to the other device that includes the current location (DH); a network interface that is programmed to receive a location of a responder through a network connection, and a display that is configured to display the location of the responder on the computing device (DI); a network interface that is configured to receive information indicating that no responders are currently available for a user of a computing device, and an output subsystem that is configured to output a warning message on the computing device that no responders are available (DJ); a network interface that is configured to establish, before initiating a communication session and at a computing device, peer-to-peer network connections with a plurality of other devices associated with candidate responders, a status module that is programmed to obtain using the network connections, current status information for a plurality of candidate responders, and a display that is configured to display the current status information for a plurality of candidate responders (DK); a network interface that is configured to establish, before initiating two-way audiovisual communication session and at a computing device, peer-to-peer network connections with a plurality of other devices associated with candidate responders, a status module that is programmed to obtain using the network connections, current status information for the candidate responders, and a display that is configured to display the current status information for the candidate responders (DL); a network interface that is configured to receive, from a responder computing device, instructions to perform one or more operations, a permissions module that is configured to determine whether the responder computing device is permitted to remotely control operation of the computing device, and a processor that is configured to perform, based on the determining, the one or more operation (DM); a display that is programmed to display a map that depicts geographically associated crime information (DN); a display that is programmed to display a map that depicts geographically associated crime information, a network in-

terface that is programmed to receive, in real-time and while displaying the map, new crime information, wherein the map is updated to additionally depict the new crime information, and an output subsystem that is programmed to output, when the new crime information is within a threshold distance, a notification (DO); a network interface that is programmed to: transmit a request to a computer system for a network address of another computing device, receive the network address, and establish, using the network address, a peer-to-peer network connection with the other computing device (DP); a user interface that is configured to receive input to connect to each member of a group of users, and a network interface that is programmed to obtain network addresses for devices associated with the members of the group of users, and sending messages requesting initiating network connections with the devices using the network addresses (DQ); an interface through which the mobile computing device acts as a user device in personal emergency response system, an input interpreter that is programmed to determine that an input received through the interface is one of a plurality of designated inputs to initiate communication with an emergency response system, and a network interface that is programmed to initiate, based on the determining, communication with the emergency response system (DR); an in-home mount, a mobile computing device that is sized to fit within the in-home mount, the mobile computing device including: a camera, a video recording module that is programmed to record video using the, and a network interface that is programmed to transmit the video to a computer system with additional data obtained by the mobile computing device (DS); a network interface that is programmed to obtain status information for a one or more users that are associated with one or more computing devices, and an output subsystem that is programmed to output the status information (DT); a network interface that is programmed to receive location information for a user associated with a computing device, a location tracking module that is programmed to determine, using the location information, whether the user has crossed over a boundary of a defined geographic area, and an alert module that is programmed to output an alert in response to the determining (DU); a network interface that is configured to provide security features to computing devices operating across a plurality of different computing platforms and operating systems (DV); a network interface that is programmed to receive, from a responder device, instructions to contact a friend of a user, a contact identification module that is programmed to identify an appropriate friend to contact, and wherein the network interface is further programmed to initiate a communication session with a computing device associated with the identified friend (DW); a security module that is programmed to encrypt real-time data with associated metadata that identifies when, where, or by whom the real-time data was collected, and a network interface that is programmed to transmit the real-time data (DX); a central computer system compris-

es a professional emergency response system (DY); a subscription module that is programmed to gate access to one or more security features based on subscription levels for users (DZ); a text messaging module that is programmed to send and receive text messages with other computing devices, and a user interface that is programmed to display the text messages on the computing device (EA); a wireless transceiver that is configured to detect nearby wireless signals from other devices, and a network interface that is programmed to transmit information regarding the detected wireless signals and the other devices (EB); a display that is programmed to display a map that depicts color coded regions that correspond to users who have begun using a mobile security application based on a recommendation from the user that was either directly or indirectly provided to the users (EC); a network interface that is programmed to receive a current location for a user, and a safety module that is programmed to determine a current safety level for the user at the current location based on one or more factors (ED); wherein a communication protocol that is used comprises webRTC (EE); a responder selection module that is programmed to select, from among a plurality of responders, one or more responders based, at least in part, on user-generated ratings for the plurality of responders (EF); a user interface that includes a graphical element comprising a slider through which a user can browse a group of users through linear swiping inputs (EG); a user interface that is programmed to receive a request to transmit a location to another computing device, a location unit that is programmed to determine the location of the computing device, and a network interface that is programmed to transmit the location to another computing device (EH); a data source from which user contact information and location information is obtained comprises social media (EI); a user interface that is programmed to receive input describing an incident, an input subsystem that is configured to collect additional details detected or sensed by the mobile computing device regarding the incident, and a network interface that is programmed to report the incident using the input and the additional details (EJ); information regarding a user is stored as a user profile (EK); and a display that is configured to display a video instructing a user how to operate a mobile security application (EL).

[0011] The features CM-EL can be combined in any of a variety of appropriate ways, including with the features A-CL. For example, the features A-EL, including all possible subsets thereof, can be used in every possible combination and in every possible permutation.

[0012] In one implementation, a computer-implemented method includes determining a location of a mobile computing device using one or more of a plurality of data sources; identifying a plurality of candidate responders; selecting a particular candidate responder based, at least in part, on one or more factors; and initiating two-way audiovisual teleconferencing between the mobile computing device and the particular candidate responder

over a network connection. The method can include one or more of the following features, which can be used in any possible combinations. The network connection can be a peer-to-peer connection. The factors can include one or more of the following: user location, responder location, responder ratings, responder skills/training, type of situation, and a predefined list of responders. The data sources include one or more of the following: GPS, WiFi, beacon signals, other data transmitted by radiofrequency that is useable to electronically locate a device. Receiving a geographic location for a user, and determining, using a database of locations and corresponding licensure status, whether said user is located within one or more licensed jurisdiction. Determining or receiving a geographic location for a user, and identifying, using a database of locations and corresponding responders, one or more appropriate responders based, at least in part, on said geographic location. Receiving a request to connect a mobile computing device with a responder service, identifying an appropriate responder service based on the location of the mobile computing device, and initiating contact with the appropriate responder service on behalf of the mobile computing device. Receiving, at a computing device, a location of a responder through a network connection; and displaying the location of the responder on the computing device. Receiving information determining whether responders are currently available for a user of a computing device; and if no responders are currently available, taking an appropriate action. Establishing, before initiating a communication session at a computing device, peer-to-peer network connections with a plurality of other devices associated with candidate responders; and obtaining and displaying, using the network connections, current status information for a plurality of candidate responders. Recording video using one or more cameras that are accessible to a computing device; modifying the video by adding one or more features; and transmitting the modified video with the features to a remote storage system for persistent storage. Receiving a current location for a user; and determining a current safety level for the user at the current location based on one or more factors.

[0013] In another implementation, a computing device includes a geographic location unit that is programmed to determine a location of a mobile computing device using one or more of a plurality of data sources; a mobile security application that is programmed to identify a plurality of candidate responders and to select a particular candidate responder based, at least in part, on one or more factors; a camera; a network interface that is programmed to transmit real-time video recorded by camera to another computing device associated with the particular candidate responder over a network connection, and to receive real-time video recorded by the other computing device; and a display that is programmed to display, concurrently with transmitting the real-time video, the real-time from the other computing device.

[0014] In another implementation, a computer-imple-

mented method includes communicating, by a mobile computing device, with another computing device as part of a two-way video chat session over a network connection; displaying, as part of the two-way video chat session, real-time video from the other computing device while transmitting real-time video from the mobile computing device to the other computing device; receiving a request to connect a mobile computing device with a responder service; identifying an appropriate responder service based on the location of the mobile computing device; initiating contact with the appropriate responder service on behalf of the mobile computing device; recording video using one or more cameras that are accessible to a computing device; modifying the video by adding one or more features; and transmitting the modified video with the features to a remote storage system for persistent storage. The method can include one or more of the following features, which can be used in any possible combinations. Receiving, at a computing device, a location of a responder through a network connection; and displaying the location of the responder on the computing device. Receiving information determining whether responders are currently available for a user of a computing device; and if no responders are currently available, taking an appropriate action. Establishing, before initiating a communication session at a computing device, peer-to-peer network connections with a plurality of other devices associated with candidate responders; and obtaining and displaying, using the network connections, current status information for a plurality of candidate responders. Receiving a current location for a user; determining a current safety level for the user at the current location based on one or more factors. A communication protocol that is used comprises webRTC. Encrypting, by a computing device, real-time data with associated metadata that identifies when, where, or by whom the real-time data was collected; and transmitting the real-time data.

[0015] In another implementation, a computer-implemented method includes determining a location of a mobile computing device using one or more of a plurality of data sources; communicating, by the mobile computing device, with another computing device as part of a two-way video chat session over a first network connection, the communicating including transmitting the location of the mobile computing device; displaying, as part of the two-way video chat session, real-time video from the other computing device; recording video using one or more cameras that are accessible to the mobile computing device; and transmitting, over a second network connection, the video to a remote storage system for persistent storage.

[0016] The method can optionally include one or more of the following features. The method can further include identifying from a data source a plurality of potential responder computing devices associated with candidate responders; and automatically selecting a particular potential responder computing device to communicate with

that is associated with a particular potential candidate responder based, at least in part, on one or more factors including the availability of the responder for communication. The method can also include receiving, at the mobile computing device, a location of a responder through a network connection; and displaying the location of the responder on the mobile computing device. The method can additionally include receiving information that indicates whether responders are currently available for a user of the mobile computing device; and if it is detected that no responders are currently available, taking an appropriate alternate action. The method can further include establishing, before initiating the communication session at the other computing device, network connections with a plurality of other devices associated with candidate responders; and obtaining and displaying, using the network connections, current status information for a plurality of candidate responders. The method can also include receiving, at the mobile computing device and from a responder computing device, instructions to perform one or more operations; determining whether the responder computing device is permitted to remotely control operation of the mobile computing device; and if the responder computing device is permitted to remotely control operation of the mobile computing device based on the determining, performing, the one or more operations. The method can additionally include encrypting, by the mobile computing device, real-time data with associated metadata that identifies when, where, or by whom the real-time data was collected; and transmitting the real-time data. The method can also include receiving a current location for a user; and determining a current safety level for the user at the current location based on one or more factors including the location. A communication protocol that is used comprises webRTC.

[0017] In another implementation, a computing device includes one or more cameras that are programmed to record video; a geographic location unit that is programmed to determine a location of a computing device using one or more of a plurality of data sources; a network interface that is programmed to communicate with another computing device as part of a two-way video chat session over a first network connection and to cause the video to be transmitted, over a second network connection, to a remote storage system for persistent storage, the location of the computing device being sent over the first and second network connections; and a display that is programmed to display, as part of the two-way video chat session, real-time video from the other computing device.

[0018] The computing device can optionally include one or more of the following features. The computing device can further include a security application that is programmed to identify a plurality of candidate responders and to select a particular candidate responder based, at least in part, on one or more factors, wherein the particular candidate responder is associated with the other computing device. The network interface can be further

be programmed to establish, before initiating the communication with the other computing device, network connections with a plurality of other computing devices associated with candidate responders; the device can further include a status module that is programmed to obtain, using the network connections, current status information for a plurality of candidate responders; and the display can further be programmed to display the current status information for a plurality of candidate responders. The network interface can further be programmed to receive, from a responder computing device, instructions to perform one or more operations; the computing device can further include a permissions module that is programmed to determine whether the responder computing device is permitted to remotely control operation of the computing device; and a processor that is configured to perform, based on the determining, the one or more operations.

[0019] In another implementation, a computer-implemented method can include determining a location of a mobile computing device using one or more of a plurality of data sources; identifying a plurality of candidate responders; automatically selecting a particular candidate responder based, at least in part, on one or more factors including the availability of the candidate responders; and initiating two-way audiovisual teleconferencing between the mobile computing device and the selected particular candidate responder over a network connection.

[0020] The method can optionally include one or more of the following features. The method can further include determining or receiving a geographic location for a user; identifying, using a database of locations and corresponding responders, one or more appropriate responders based, at least in part, on the geographic location; receiving a request to connect the mobile computing device with a responder service; identifying an appropriate responder service based on the location of the mobile computing device; and initiating contact with the appropriate responder service on behalf of the mobile computing device. The method can further include receiving a geographic location for a user; and determining, using a database of locations and corresponding licensure status, whether the user is located within one or more licensed jurisdictions. The method can also include receiving, at the mobile computing device, a location of a responder through a network connection; and displaying the location of the responder on the mobile computing device. The method can additionally include establishing, before initiating a communication session at a computing device, a plurality of network connections relating to a plurality of other devices associated with candidate responders; and obtaining and displaying, using the network connections, current status information for said plurality of other devices associated with candidate responders. The method can also include receiving information identifying whether responders are currently available for communication with a user of a computing device; and in response to detecting that no responders are currently

available, taking an appropriate alternate action. The method can additionally include receiving a current location for a user; and determining a current safety level for the user at the current location based on one or more factors including said location for a user.

[0021] The details of one or more implementations are depicted in the associated drawings and description thereof below. Certain implementations may provide one or more advantages. For example, the disclosed technologies can increase security, particularly personal safety, by connecting a person or group of people at risk to responders who can help. For instance, in a crime scenario the disclosed technology can be effective at stopping or averting a crime, dissuading an attacker, and/or capturing information about the attacker, situation, and/or location that will enhance emergency personnel's ability to stop, apprehend, and/or prosecute a criminal. In a medical emergency scenario, the disclosed technology can be effective at providing real time medical information, 2-way or multi-way video, and/or capturing information about the victim, situation, and/or location that will enhance emergency personnel's ability to administer emergency care. In an accident (e.g., auto accident) or lost person scenario, the disclosed technology can aid in capturing information about the location of the person and/or other information helpful in bringing about their rescue.

[0022] In another example, before initiating a security session with a responder or other user, a user can be provided with assurances that someone is readily available to help him/her by preemptively initiating connections between the user's mobile computing device and the computing devices of other user(s) before the user has requested assistance/help. The state of such preemptive connections can be part of a Ready Mode and can allow for a user to quickly engage an available responder for assistance. Users can be notified of which other users and responders are available through user interface features, such as status indicators for a group of other users and responders, which can provide assurances of a user's available and readily deployable options for assistance.

[0023] In a further example, remote control of another user's mobile computing device can help and provide assistance to the other user in a variety of contexts. For instance, in a crime scenario such another user may not be able to activate his/her mobile computing device to obtain help from a remote user/responder. Remote activation can allow for such assistance and help to be provided. In emergency scenarios, remote activation can allow for a variety of details regarding a user's location and state to be obtained, including capturing live audio and video from the user's device and including the ability to initiate or control all of the same functions that the user himself could control on his device, which may be crucial for deploying medical personnel to an appropriate location to provide assistance.

[0024] In another example, a user needing assistance

can automatically be routed to a responder who is best able to assist the user with minimal input from the user. For example, multiple factors can be considered when pairing a user in need of assistance with an appropriate responder, such as proximity of responders to the user, ratings of the responders by previous users, a type of situation (e.g., emergency, crime), user profile information and preferences, current availability of responders, responder skills and training, the group of the responder (e.g. responder is member of local police, responder is responsible for a particular jurisdiction, responder is member of private security for a particular organization), and/or other factors. Based on such factors, a user can be automatically paired with a responder who is able to best assist the user, which can improve the likelihood of a positive outcome for the user.

[0025] In a further example, by automatically sending out confirmation messages to other users/responders once a user has arrived at a destination location (for example the user's home, work, or another safe location), a user's safe arrival can be confirmed to other users (for example to the user's friends or family). Additionally, the absence of such messages after a period of time when arrival by the user at a destination was expected can allow for actions to be taken to assist the user, for example to send out notification messages to responders or friends/family, which can reduce the response time of someone helping the user and increase the likelihood of a positive result for the user.

[0026] In another example, by providing users with updated safety scores for their surroundings based on a variety of factors, many of which would not be readily apparent to users from their physical surroundings, users can be better alerted of potentially dangerous situations and can take preventative steps to avoid any harm or danger from befalling them. For example, when a user enters a geographic area that has high crime rates and within which a recent incident report was received from another user, a safety score for that user can be provided to the user or to other users (including the user's friends, family, or responders) indicating that he/she is in an unsafe location and can suggest a route to a safer location.

[0027] In a further example, the disclosed technology can aid users in sending detailed and informative text messages to appropriate emergency responder systems (e.g., a private security company, public security company, 911 / PSAP systems), which can allow for users to quickly and silently request assistance. For example, in some instances a user may not want to initiate a video chat session or phone call with an emergency responder, such as when the user is hiding from an assailant or when there is a large amount of background noise that would render video/audio interaction useless. The disclosed technology can allow users in such situations to still obtain assistance when needed.

[0028] Other features, objects, and advantages of the technology described in this document will be apparent from the description and the drawings, and from the

claims.

Brief Description of the Drawings

[0029]

FIG. 1 is a conceptual diagram of an example computer system for providing security features on an example mobile computing device.

FIG. 2 is a diagram of an example system for providing security features on a mobile computing device.

FIG. 3 is a flowchart depicting an example technique for assisting a user of a computing device.

FIG. 4 is a flowchart of an example technique for initiating contact between a user's device and a responder.

FIGS. 5A-F are flowcharts of an example technique for communicating between a user device and a responder device as part of a security session.

FIG. 6 is a flowchart of an example technique for facilitating auto-answer features between a user device and a responder device.

FIG. 7 is a flowchart of an example technique for providing emergency text messaging services on a user device.

FIG. 8 is a flowchart of an example technique for providing real-time crime maps and safety levels to users.

FIGS. 9A-F are screenshots of user interfaces that can be presented on computing devices.

FIG. 10 is a screenshot of a user interface that can be presented on computing devices in Ready Mode.

FIGS. 11A-E are screenshots of a user interface that can be presented on computing devices when transitioning from Ready Mode to Caller Mode and Responder Mode.

FIGS. 12A-D are screenshots of a user interface that can be presented on computing devices to initiate and participate in two-way instant messaging.

FIG. 13 is a screenshot of a user interface that can be presented on computing devices to access several security-related features.

FIG. 14 is a screenshot of a user interface that can be presented on computing devices to display and access several security-related features.

FIG. 15 is a screenshot of a user interface that can be presented on computing devices during a 2-way video chat.

FIG. 16 is a screenshot of a user interface that can be presented on computing devices to display and access several security-related features.

FIG. 17 is a screenshot of a user interface that can be presented on computing devices to report an incident.

FIGS. 18A-B are a screenshot of a user interface through which a user can enter their profile information and register to use the security features dis-

cussed above.

FIG. 19 is a screenshot of a user interface that depicts a safety level indicators.

FIG. 20 is a screenshot of an example home screen for a mobile security application.

FIG. 21 is a screenshot of an example user interface through which a user can enter and transmit a text message to emergency responders.

Definitions

[0030] Substantially Immediate/Substantially Immediately, as used herein, refers to a short period of time between process steps. For example, if one process follows another preceding processes substantially immediately, the following occurs within a time period of less than X seconds, such as within a period of time less than X=300, 60, 30, 10, 5, 4, 2, 1, 0.5, 0.2, 0.1, 0.01, 0.001, 0.0001, 0.00001, 0.000001 seconds or less. Live connection or live video may mean video that is seen by the remote peer substantially immediately relative to the time that it is captured (e.g., when a single frame is captured by a caller, it is seen within 300, 60, 30, 10, 5, 4, 2, 1, 0.5, 0.2, 0.1, 0.01, 0.001, 0.0001, 0.00001, 0.000001 seconds or less by the responder). In Ready Mode, available instantly may mean that a live connection may be established substantially immediately.

[0031] Substantially real time, as used herein, refers to a short period of time between process steps. For example, something occurs in substantially real time if it occurs within a time period of less than X seconds, such as within a time period of less than X=300,60,30, 10,5, 4, 2, 1, 0.5, 0.2, 0.1, 0.01, 0.001, 0.0001, 0.00001, 0.000001 seconds or less.

Detailed Description

[0032] This document generally describes computer-based technology for providing security features that are readily accessible to users of computing devices, such as mobile computing devices. A variety of different security features are described below with regard to the figures.

[0033] FIG. 1 is a conceptual diagram of an example computer system 100 for providing security features on an example mobile computing device 102. In particular, in the depicted example the mobile computing device 102 enters Ready Mode through preemptive communication with one or more other computing devices 108a-d and initiates a video communication session with one or more of the other computing devices while simultaneously transmitting video and other data to a remote data storage system 106 for secure storage 130.

[0034] The depicted computer system 100 includes the mobile computing device 102 that communicates over a network 104 with a data storage computer system 106 and a plurality of other computing devices 108a-d. The mobile computing device 102 can be any of a variety of

appropriate mobile computing device, such as a smartphone, a PDA, a tablet computing device, a laptop, a wearable computing device (e.g., GOOGLE GLASS, smartwatches), a computing device embedded within a vehicle (e.g., embedded automobile computer system, truck, car, airplane, bus, helicopter, boat), and/or other appropriate mobile computing device. In some implementations, the mobile computing device 102 can be a non-mobile computing device, such as a desktop computer.

[0035] The network 104 can be any of a variety of appropriate networks over which the mobile computing device 102 can communicate with the data storage computer system 106 and/or the other computing devices 108a-d, such as the internet, local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), mobile data networks (e.g., 4G wireless networks), wireless networks (e.g., Wi-Fi networks, BLUETOOTH networks), peer-to-peer connections, TCP/IP, UDP, secure networks such as HTTPS, or any combination thereof.

[0036] The data storage computer system 106 can be any of a variety of appropriate computer system with associated storage devices, such as cloud-based computer systems with associated data storage subsystems. The other computing devices 108a-d can be any of a variety of appropriate computing device and/or computer system, such as mobile computing devices, desktop computers, and/or computer servers.

[0037] As depicted in FIG. 1, the mobile computing device 102 is associated with a user 110 who is faced with a possible dangerous situation or person 112, which can include any of a variety of dangers or emergencies such as another person (e.g., aggressor, criminal), a medical emergency, an accident (e.g., automobile accident), and/or other dangerous physical situations.

[0038] Even before the user 110 is faced with the possible danger 112, the mobile computing device 102 can preemptively establish connections with the data storage system 106 and/or some or all of the other computing devices 108a-d over the network 104, as indicated by step A (114). These preemptive connections can be part of Ready Mode, which the user 110 may toggle on/off through one or more settings on the mobile computing device 102. As part of Ready Mode, the mobile computing device 102 periodically (e.g., every second, every 5 seconds, every 10 seconds) provides to and receives status information (e.g., active, inactive, user presently interacting with the mobile computing device 102) from the other devices 106 and 108a-d. This status information can indicate whether a user/service associated with a corresponding device is presently available to participate in a security session. For example, status information for the data storage system 106 can indicate whether recording of information obtained by the mobile computing device 102 (e.g., video, audio, location information, sensor data) can be instantly initiated (e.g., initiated with less than a threshold delay) by the data storage system 106.

[0039] Each of the other computing devices 108a-d can be associated with one or more different entities, such as the example entities depicted in FIG. 1. For example, the computing device 108a is depicted as being associated with acquaintances 116a (e.g., friends, colleagues, family members) of the user 110, the computing device 108b is depicted as being associated with a professional security service 116b (e.g., non-government groups/companies that provide security services), the computing device 108c as being associated with an emergency response system 116c (e.g., 911/PSAP system), and the computing device 108d is depicted as being associated with emergency responders 116d (e.g., police officers, fire fighters, emergency medical service providers, military).

[0040] Through the preemptively established connections with these devices 108a-d, status information for users associated with the entities 116a-d can be obtained. The status information can indicate any of a variety of details regarding the availability of the computing devices 108a-d and/or associated entity users 116a-d to participate in a security session with the user 110 and the mobile computing device 102. For example, the status information can indicate whether users are currently at or away from the computing device 108a-d, which can be determined by the computing devices 108a-d based on any of a variety of information, such as whether the users are currently providing input to the computing devices 108a-d (e.g., typing, clicking on screen elements, having an app in the foreground of the device, moving a pointer device) and/or whether the users are visible through a camera of the computing devices 108a-d. In another example, the status information may include a current video feed from the computing devices 108a-d so that the user 110 can verify whether the users for entities 116a-d are currently available to provide assistance. Such a video feed may be provided at a lower level of quality (e.g., lower frame rate, lower resolution) than typically provided during video chat sessions, so as to minimize the bandwidth consumed from the transmission. In another example, the status information may include the person's location or distance from the user.

[0041] The mobile computing device 102, during Ready Mode, can display information that identifies the available entities and status information for them, as indicated by step B (118). For example, the mobile computing device 102 can display a map that includes icons identifying the location of the computing devices 108a-d and their associated users 116a-d relative to a location of the mobile computing device 102, as well as their current status information. These icons may include photos of the associated users, when they were last connected, when they last changed position, or their computed safety level or other information. In another example, the mobile computing device 102 can display a list of the computing devices 108a-d, their corresponding users 116a-d, and their corresponding status information. In another example, the mobile computing device 102 can present a pre-

view of a video that would be provided to the data storage system 106 for recordation along with an indicator (e.g., blinking light/icon) as to whether the data storage system 106 is available to instantaneously begin recordation of such data, and whether such recording has started or is ongoing. In some implementations, when no entities are available for the user 110, the mobile computing device can provide a notification that no responders are available to help and can additionally provide one or more alternative channels of assistance, such as dialing emergency response services (e.g., 911 service, campus police).

[0042] The information regarding the computing devices 108a-d and their corresponding entities 116a-d can be presented in a selectable manner on the mobile computing device 102 such that the user 110 can select one or more of the entities 116a-d for a security session (e.g., video communication and data recordation at the data storage system 106) or other communication session (e.g., messaging communication system).

[0043] The mobile computing device 102 can monitor for and detect input that indicates an intention of the user 110 to initiate a security session, as indicated by step C (120). Such input can take any of a variety of forms. For example, a user can select a graphical user interface feature (e.g., icon, virtual button) or physical button on the mobile computing device 102, or on another device connected to the mobile computing device 102 by wired or wireless connection (e.g., wearing watch or piece of jewelry with an embedded button to activate the app), provide audible input (e.g., utter a particular phrase), and/or provide motion based input (e.g., shaking the device) that is associated with initiating a security session. In another example, the absence of input for a period of time may indicate such an intention (e.g., holding the device in a particular orientation and/or pose for at least a threshold period of time, pressing a button down for at least a threshold period of time before releasing it). In another example, detected motion that is indicative of the user 110 losing control of the device 102 (e.g., dropping the device 102) and/or being involved in a physical altercation (e.g., automobile accident, physical scuffle) can be identified by the mobile computing device 102 as input to initiate a security session. In another example, detected motion such as a change in velocity (for example when a car abruptly stops, potentially indicating an accident) can be identified by the mobile computing device 102 as input to initiate a security session.

[0044] In response to detecting the input, the mobile computing device 102 can automatically initiate a security session with one or more of the computing devices 108a-d and the data storage system 106, as indicated by step D (122). In instances where the user 110 has not selected one of the computing devices 108a-d to communicate with, the mobile computing device 102 itself can automatically select one or more of the computing devices 108a-d with which to initiate the security session based on a variety of factors, such as proximity to the

mobile computing device 102, ratings associated with the corresponding entities 116a-d, expertise and skills for the corresponding entities 116a-d, an indication of the type of possible danger 112, predefined preferences for the user 110, one or more lists/rankings of entities 116a-d as designated by the user 102, presence within one or more emergency response jurisdictions, sensor data, or any combination thereof. Other appropriate factors can also be used. In other words, if the user is associated with a whole group of potential connection recipients, for example a whole group of potential responders, the device 102 can automatically select an appropriate potential connection recipient based on a number of factors such as proximity to the user, and initiate a connection.

[0045] As part of the security session, the mobile computing device 102 can concurrently transmit audio, video and other data to the data storage system 106, as indicated by step E (124), and can participate in a video communication session with one or more of the computing devices 108a-d, as indicated by step F (126), potentially simultaneously. The data storage system 106 can receive a stream of real-time audio, video and other data (e.g., location information, sensor data, identity of other computing devices located nearby the mobile computing device 102), and can store the data, as indicated by step G (128). The data can be stored in one or more secure storage devices 130 to which access is restricted. For example, the data can be encrypted and stored in the secure storage devices 130, and read/write/delete privileges can be restricted such that, other than administrators of the data storage system 106, no users are able to modify the data written to the secure storage devices 130. For instance, the user 110 is not able to delete data that is uploaded to the data storage system 106 and stored in the secure storage devices 130.

[0046] The data stored in the secure storage devices 130 can be stored in a manner that will permit for the data to be used as evidence, sufficient for admission before a judicial or administrative body, of events that took place between the user 110 and the possible danger 112. As such, the data storage system 106 may trace and record information regarding a communication route over the network 104 between the mobile computing device 102 and the data storage system 106, as indicated by step H (131). Additionally, the data storage system 106 may also obtain and store raw data from the mobile computing device 102, such as raw GPS data and/or raw sensor data (e.g., motion sensor data), in addition to synthesized information from the mobile computing device 102 (e.g., geographic location determined by the mobile computing device 102). The secure storage devices 130 can store a variety of pertinent data from the mobile computing device 102, such as video/audio files, images, trace routes, location data, sensor data, and/or other appropriate data. The data being transmitted may also allow secure communication and encryption of data, as well as verification of the user transmitting the data, and the time and location from where it was transmitted. For ex-

ample, the data being transmitted can be encrypted along with a username, password, time, location, biometrics, public or private cryptographic key, other security identifiers, or other information. This information may also be encrypted and or stored for verification using a blockchain-based methodology or other approaches derived from cryptography and cryptocurrencies (e.g. bitcoin, etherium). The information being transmitted can be encrypted or stored to be only accessible or readable to the user himself, or to someone with appropriate security information. The privacy of the user, or the user's identity, can also be secured and maintained cryptographically. These encryption steps may be performed locally on the mobile device of the user. These encryption steps may be performed on the responder device. These encryption steps may be performed on a remote server.

[0047] During the established video communication session, the mobile computing device 102 can transmit, to one or more of the devices 108a-d, real-time video, audio, text or message information, and/or image data, as well as location updates, information identifying the mobile computing device 102 and/or the user 110, information that may identify another user who may be causing the possible dangerous situation (e.g., images, audio, video of the other user; detected other computing devices that are located near mobile computing device 102), and/or other appropriate information. Each of the computing devices 108a-d can additionally provide similar information to the mobile computing device 102. The information may be transmitted between the mobile computing device 102 and multiple devices from the computing devices 108a-d in substantially real time and/or using peer to peer or server-based connections. Video communication sessions can be between the mobile computing device 102 and multiple devices from the computing devices 108a-d. For example, the mobile computing device 102 can establish a first video communication session with one of the computing devices 108a associated with the user's acquaintances 116a and a second video communication session with the computing device 108b that is associated with the profession security service 116b.

[0048] In addition to transmitting real-time video feeds to the mobile computing device 102, each of the computing devices 108a-d may additionally initiate remote control over the mobile computing device 102 (e.g., turn on/off various subsystems of the mobile computing device 102, such as lights, speakers, camera, microphone, display), initiate a communication session with one or more other computing devices (e.g., the acquaintance 116a can use the mobile computing device 108a to cause the mobile computing device 102 to communicate with the computing device 108c corresponding to the emergency response system 116c), and/or broadcast information from the video communication session to other users/devices (e.g., transmit current location and real-time video/audio feed to a nearby emergency responder 116d). Some of the entities 116a-d may have additional

subsystems to further facilitate such assistance to the user, such as the professional security service 116b which can have access to emergency routing data 134 (e.g., information identifying an appropriate emergency response system (e.g., 911 or PSAP system or jurisdiction) to handle the user's 110 situation), user data 136 (e.g., information about the user 110, such as height, weight, name, age, appearance, address, automobile, medical conditions, preferences), and a secure data storage system 138 (e.g., storage system to log information regarding the interaction between the mobile computing device 102 and the computing devices 108a-d). Although not depicted, others of the computing devices 108a and 108c-d may either have data repositories similar to 134-138, or may have access to such information.

[0049] While the transmitting data to the data storage system 106 (step E) and participating in the video communication session (step F), the mobile computing device 102 can concurrently output the real-time audio and video received through the video communication session from the one or more of the computing devices 108a-d, as indicated by step I (140). Such outputting of the video can allow for a remote user (e.g., entities 116a-d) to virtually participate in the physical situation that is before the user 110 in an attempt to stop or mitigate the possible danger 112. For example, a person who is possibly dangerous 112 can see the video and/or hear the audio that is output on the user device 102, as indicated by video output 142, so as to provide verification that someone outside of the physical situation is monitoring and involved in the situation, as indicated by line 152 indicating that the video output 142 and the audio output 150 are presented to the possible danger 112. An example video output 142 on the display of the mobile computing device 102 is depicted as including textual information 144 identifying the remote user ("Police Officer"), a live video feed 146 that shows the remote user (police officer), additional information 148 that the remote user has directed (e.g., through remote control) the mobile computing device to display 102. In the example, one of the other computing devices 108a-d that is participating in the video chat (video chat can be a multi-way (e.g., two-way, three-way, four-way) videoconference) can provide an image of the possible aggressor 112, which was obtained by the other computing device through the video communication session 126. The image of the possible aggressor 112 can serve as proof to the possible aggressor 112 that his image has been recorded, so as to imply that he/she is likely to get caught and should cease all aggression toward the user. Additionally, an audible message 150 can be output by the speakers of the mobile computing device 102.

[0050] For example, the user 110 can hold the mobile computing device 102 to be facing the possible aggressor 112 so that the possible aggressor 112 can see and hear the police officer (remote user) addressing him/her (for example the possible aggressor 112 can see the display 142). The police officer (remote user) can cause the mo-

bile computing device 102, through remote device control, to present information to the possible aggressor 112, such as the textual information 144 identifying the police officer and the image 148 that provides verification that evidence of the possible aggressor 112 actions have been captured and are in the hands of the authorities. Such involvement by a remote user is likely to improve the chance of the possible dangerous situation 112 ending without anything having happened to the user 110. Examples of other actions that a remote user, like the police officer in the example, can cause the mobile computing device 102 to take include turning on/off a light source (e.g., flash) on the mobile computing device, activating an alarm on the mobile computing device (e.g., audible alarm or pre-recorded audio or voice message, for example 'Help!'), and/or displaying the location of an emergency responder who is en route to the user's location.

[0051] The disclosed operations that are described above as being performed by the mobile computing device 102, the data storage system 106, and the computing devices 108a-d, can be implemented in any of a variety of appropriate ways on the devices/systems, such as through software (e.g., mobile device applications, operating system features), hardware (e.g., application specific integrated circuits (ASICs)), firmware, or any combination thereof.

[0052] FIG. 2 is a diagram of an example system 200 for providing security features on a mobile computing device 202. The example system 200 is depicted as including the mobile computing device 202, other mobile computing devices 204, computer systems 206 associated with professional security and/or emergency response systems, a data storage system 208, a central computer system 210, other computing devices 212 that are available to output audio or video information, a network 214, and wearable computing or monitoring devices 216. The mobile computing device 202 can be similar to the mobile computing device 102 described above with regard to FIG. 1. The other mobile computing devices 204 can be similar to the computing devices 108a and 108d described above. The computer system 206 can be similar to the computing devices 108b-c. The data storage system 208 can be similar to the data storage system 106. The network 214 can be similar to the network 104.

[0053] The mobile computing device 202 includes an input subsystem 216 and an output subsystem 218 through which input and output can be provided to users by the mobile computing device 202. The input subsystem 216 includes a touchscreen 220a (e.g., touch sensitive display, touch sensitive surface, touch sensitive housing, presence sensitive surface), keys and/or buttons 220b, microphone(s) 220c, motion sensors 220d (e.g., accelerometers, gyroscopes), camera 220e (e.g., rear-facing camera, forward-facing camera, 3D cameras), and/or other appropriate technologies. In some implementations, the cameras 220e can additionally or alternatively detect portions of the electromagnetic spec-

trum that are outside of the range of visible light, such as infrared radiation. The output subsystem 218 includes a display 222a (e.g., LCD display, LED display), speakers 222b, a projector 222c, haptic devices 222d (e.g., vibration generating devices, tactile displays), light sources 222e (e.g., flash bulb, night vision or infrared energy), and/or other appropriate technologies. In some implementations, portions of the input and output subsystems 216 and 218 can be configured to provide additional inputs and outputs on the mobile computing device 202. For instance, the speakers 222b can be configured to output ultrasonic and/or subsonic sound waves, the reverberation of which can be detected by the microphone(s) 220c to provide sonar detection capabilities. Similarly, the device may use radar or night vision capabilities.

[0054] The mobile computing device 202 additionally includes wireless transceivers 224 for communicating over one or more wireless communication technologies. For example, the wireless transceivers 224 can include one or more appropriate wireless transceivers, such as wireless radio transceivers like Wi-Fi transceivers, short-range wireless transceivers (e.g., BLUETOOTH transceivers), cellular network transceivers, NFC, and/or mobile data network transceivers (e.g., 3G/4G transceivers). The mobile computing device 202 can additionally include a location module 226 that is programmed to determine a location of the mobile computing device 202 either in terms of absolute positioning (e.g., GPS position data, latitude and longitude) or relative positioning (e.g., positioning relative to particular fixed objects or inside buildings including cell tower, WiFi hotspots or networks, other radio networks, satellites). The location module 226 may include a GPS unit 228a that is programmed to detect GPS satellite signals and, based on the detected signals, to determine a geographic location of the mobile computing device 202. The location module 226 may also include a micro-location unit 228b that is programmed to determine the location of the mobile computing device 202 with a greater level of granularity than the GPS unit 228a and/or in situations where the GPS unit 228a is unreliable (e.g., interior locations). The micro-location unit 228a can use signals received through the wireless transceivers 224, such as signals from Wi-Fi networks and/or beacon signals, to determine either absolute or relative positioning of the mobile computing device 202.

[0055] The mobile computing device 202 additionally includes a CPU 230 (e.g., single core, dual core, quad core) that is programmed to execute instructions 232 (e.g., binaries, object code, scripts) that are stored/loaded into memory 234 (e.g., RAM, ROM). The CPU 230 can execute instructions of any of a variety of types to provide security features on the mobile computing device 202, such as executing instructions to cause the mobile computing device 202, through its component parts, to initiate a session with one or more of the other computing devices 204 and/or professional security/emergency re-

sponse systems 206, while concurrently transmitting data for secure storage to the data storage system 208. The mobile computing device 202 can additionally include one or more portable power source 236 (e.g., a battery) or backup power sources, or power connections (e.g. to an outlet), or solar or other power inputs.

[0056] Although not depicted, the mobile computing device 202 can be provided with an appropriately sized holster/case/sleeve that is designed to receive and hold the mobile computing device 202. This case may hold the device in such a manner that the input and output subsystems 216 and 218, respectively, will be able to obtain information about the user's surroundings and convey information from remote users to other people located near the user while at the same time being worn by the user, so as to provide the user with hands free operation of the mobile computing device 202. For example, the holster/case/sleeve can be a lanyard type apparatus that is worn about around a user's neck and that holds the device in a steady position near a center of the user's chest. In another example, the holster/case/sleeve can include a clip or strap that allows for the device to easily be secured to clothing, bags, appendages, or other objects. In another example, the holster/case/sleeve can include a clip or strap that allows for the device to easily be secured to a surface such as the surface of a helmet worn by the user, a vehicle or vehicle windshield, bicycle, or other piece of equipment. The holster/case/sleeve can additionally include a reserve power source (e.g., additional batteries) that can extend the duration during which the mobile computing device 202 can be used before losing power.

[0057] The mobile computing device 202 can additionally include a security module 240 that is programmed to provide security features to a user of the mobile computing device 202, including both from the perspective of a user in need of assistance, such as the user 110 described above with regard to FIG. 1, as well as a user who is providing assistance, such as the acquaintances 116a. The security module 240 can provide security features similar to those described above with regard to FIG. 1, as well as additional/alternative security features. The security module 240, and its component parts, can be implemented in any of a variety of appropriate ways, such as through software that is executed by the CPU 230 (e.g., mobile device application, operating system features), hardware (e.g., ASICs), firmware, or any combination thereof.

[0058] The security module 240 can include a ready mode unit 242a that is programmed to establish and maintain network connections with other computing devices before an intent to initiate a security session has been detected as part of Ready Mode (e.g., step A (114) described above with regard to FIG. 1). The network connections with the other computing devices can be peer-to-peer connections. Such an intent to initiate a security session can be detected by the input analyzer 242b, which is configured to determine whether the user has,

through an action (voluntary or involuntary) or omission (voluntary or involuntary), indicated an intent to initiate a security session (e.g., step B (120) described above with regard to FIG. 1).

[0059] The security module 240 additionally can include a remote control client 242c that is programmed to receive and process instructions from other computing devices (e.g., other mobile computing devices 204) to remotely control the mobile computing device 202. Before providing such remote access and control to information and components of the mobile computing device 202, such as control over the input and output subsystems 216, 218, the remote control client 242c can determine whether the requesting device and/or associated user have been given permission to have such access and control by checking against a set of permissions 242d. For example, a user may want to restrict users included on the permissions 242d to only close and trusted family members (e.g., spouse, parents, child) and friends (e.g., best friend).

[0060] The security module 240 can additionally include a routing module 242e that is programmed to determine an appropriate remote user and corresponding computing device to which to route a security session for the mobile computing device 202. The routing module 242e can select an appropriate remote user/corresponding computing device based on one or more of a variety of factors, such as proximity to the mobile computing device 202, user preferences (e.g., designation list of preferred responders), a type of situation (e.g., crime, medical emergency, natural disaster), and/or other appropriate factors. In some implementations, the routing module may alternatively be implemented at a remote computing device, such as the central computer system or server 210, which can receive a request to initiate a security session from the mobile computing device 202 and can select an appropriate other computing device for the session.

[0061] The security module 240 can store user information 242f, such as a user id, name, age, height, appearance, image, and/or preferences, which can be provided to other computing devices during security sessions. This information, for example a user profile, may also be stored on the central computer system or server 210. An identification module 242g of the security module 240 can additionally identify other users who are located around the mobile computing device through any of a variety of appropriate techniques, such as voice recognition, facial recognition, biometric identification (e.g., gate, proportions of body parts), and/or identification through nearby computing devices transmitting wireless signals (e.g., passive monitoring of wireless signals from nearby devices, active communication with such devices). The identification module 242g may use one or more data sources for such identifications, such as a user's photos, videos, social network information (e.g., friend lists, friend photos/videos, friend location, check-ins), and/or lists of contacts (e.g., telephone contact list, email

contact list). The identification module 242g may alternatively and/or additionally be implemented on one or more other computing devices that are in communication with the mobile computing device 202, such as the central computer system 210 and/or the professional security/emergency response systems 206.

[0062] A text message subsystem 242h of the security module 240 can be programmed to automatically populate and/or route a text message to an appropriate emergency responder with minimal input from a user. For example, the text message subsystem 242h can add detailed information regarding the location of the mobile computing device 202, the surrounding environment, a type of emergency, and user identity information into a text message and can ensure that the text message is directed to an appropriate responder without direction from a user.

[0063] The security module 240 can include a user interface 242i through which users can access and use the security features provided by the security module 240. The user interface 242i can present information and receive input from a user in any of a variety of appropriate ways, such as through any and all components of the input and output subsystems 216 and 218, respectively.

[0064] The security module 240 additionally includes a security session manager 242j that is programmed to manage interactions between the mobile computing device 202 and other computing devices during sessions. In particular, the security session manager 242j includes a data capture manager 242k that is programmed to capture relevant data from the components of the input subsystem 216, the wireless transceivers 224, and/or the location module 226. The security session manager 242j additionally includes a data transmission manager 242l that is programmed to transmit a stream of, as least a portion of, the data captured by the data capture manager 242k to one or more of other computing devices (e.g., the other mobile computing devices 204, security/emergency response systems 206) and to the data storage system 208.

[0065] The mobile computing device 202 includes an input/output (I/O) interface 244 that is configured to communicate over the network 214 and with the wearable computing devices 216. The I/O interface 244 can be any of a variety of appropriate interface, such as a wired interface (e.g., Ethernet card) and/or wireless interface (e.g., wireless transceivers 224, wireless chips, and antennae).

[0066] The other mobile computing devices 204 can have any of the same features as the mobile computing device 202, but may be associated with other users (e.g., acquaintances, emergency responders).

[0067] The professional security/emergency response system 206 can include some or all of the components 216-244 of the mobile computing device 202, where appropriate, and may or may not be a mobile device. The professional security/emergency response system 206 can include additional components that may not be avail-

able on the mobile computing device 202 and/or the other mobile computing devices 204, such as emergency routing data 246 and/or user data 248. The emergency routing data 246 can correlate appropriate emergency response systems with the location of the mobile computing device 202. For example, the professional security/emergency response system 206 can perform a 'PSAP dip' to determine the correct 911 dispatch center for the location of a user who may be having an emergency. This function may be performed by using a database that allows every location to be converted into the corresponding PSAP/dispatch center, and to provide contact information for that dispatch center including phone number, email number, network id, and electronic communication identification. This function may be performed by a remote server, and may be performed using a remote API. One examples of a PSAP (Public Safety Answering Point) system is the PSAP PRO system provided by PitneyBowes.

[0068] The user data 248 can be a repository of relevant information for a user of the mobile computing device 202, such as the user information 242f (or a portion thereof).

[0069] The professional security/emergency response system 206 can additionally include a secure storage device(s) 250 to securely log data received from the mobile computing device 202 and/or transmitted to the mobile computing device 202 during a security session. Although not depicted, the mobile computing device 202 and/or the other mobile computing devices can also include secure storage device(s) to redundantly log such information as well.

[0070] The data storage system 208 can include a trace module 252 that is configured to encrypt and/or verify and/or trace communication paths between the data storage system 208 and the mobile computing device 202, so as to provide a proper foundation for admissibility of logged data as evidence during judicial and/or administrative proceedings. The data storage system 208 additionally include secure storage devices 254. These encryption steps may be performed locally on the mobile device of the user. These encryption steps may be performed on the responder device. These encryption steps may be performed on a remote server.

[0071] The central computer system 210 can be used to connect the mobile computing device 202 with other appropriate devices and systems, such as the data storage system 208, the other mobile computing devices 204, and the system 206. For example, the central computer system 210 can provide IP address information for the other mobile computing devices 204 to the mobile computing device 202, which the ready mode unit 242a can use to establish peer-to-peer connections with the other computing devices 204.

[0072] The other computing or monitoring or display devices 212 can be devices that are located near the mobile computing device 202 and that have open and accessible input or output devices (e.g., display 256 and

speakers 258, camera, microphone) over which the mobile computing device 202 can stream and output information. For example, the other computing devices 212 can be televisions that have open Wi-Fi Direct access through which the mobile computing device 202 can broadcast audio and/or visual information. In another example, the other computing devices 212 can be specially designed and/or located security devices that allow for a user in distress to activate an alarm over an a wireless connection (e.g., BLUETOOTH connection). Such streaming of audio and visual information to the other computing devices 212 can help alert others in the area to the dangerous situation and can solicit their help. Streaming to such devices may be remotely controlled by a remote user, such as the users of the other mobile computing devices 204 and/or the system 206. Such other computing or monitoring or display devices 212 may also be used to record audio or video and transmit it to the network 214, the central computer system 210, or to professional security /emergency response system 206, or mobile computing device 202.

[0073] The wearable computing devices 216 can include any of a variety of appropriate wearable computing device, such as eyewear (e.g., GOOGLE GLASS), smart watches, wearable cameras (e.g. GoPro, Looxcie) and/or wearable motion sensors or biosensors (e.g. heart monitor, breathing monitor, pulsox, EEG monitor, blood composition monitor including glucose monitor). The wearable computing devices 216 can provide information to the mobile computing device 202 regarding the surrounding physical environment and/or a stat of the user, and can additionally output information. Such inputting and outputting of information can be accomplished through sensors 260 (e.g., motion sensors), camera(s) 262, speakers 264, and/or other appropriate components.

[0074] FIG. 3 is a flowchart depicting an example technique 300 for assisting a user of a computing device. Portions of the technique 300 can be performed, in whole or in part, by any of a variety of appropriate computing devices and/or systems, such as the mobile computing device 102, the other computing devices 108a-d, the data storage computer system 106, the mobile computing device 202, the other mobile computing devices 204, the professional/emergency response system 206, and/or the data storage system 208.

[0075] As an overview, the technique 300 can include one or more of the following steps, which can be performed, in whole or in part, in any of a variety of appropriate orders:

Initiate Contact (302). Initiate audio, video, two-way or multi-way contact between the mobile computing device of a user (or plurality of users) and a plurality of responders. Such contact can be over peer-to-peer connections.

[0076] Continuous Real Time Recording and Transmission of Information from User (304). Information from the user or their situation may be transmitted in substantially real time by the mobile computing device

of the user to computing devices/systems associated with the responder(s). This information may include audio/video from the user's device, photos, text messages, GPS or other localization information. All of this information may be stored locally on the user and/or responders' devices, and/or on a remote server system (e.g., data storage system 106).

[0077] Continuous Real Time Recording and Transmission of Information from Responder(s) (306). Information from the responder(s) may be transmitted in substantially real time by computing devices associated with the responders to a computing device associated with the user(s). This information may include audio/video from the responder's device, photos, text messages, GPS or other localization information. All of this information may be stored locally on the user and/or responders' devices, and/or on a server system (e.g., data storage system 106).

[0078] Remote Control of User's Device (308). The Responder(s), through their computing devices/systems, may remotely control the features of the user's device, for example to take high resolution photos using the user's device and have them sent, zoom, capture audio, adjust volume, turn on/off speaker or speakerphone, turn on/off lights, turn on/off alarms, initiate contact with other users, responders, and/or emergency services (e.g., 911 or other emergency services call) from the user's device. The remote control can allow the remote user any of the functions available locally to the user who is physically present with the device.

[0079] Help User (310). The Responder(s), through their computing devices/systems, may help the user, for example by communicating with the user or with a potential assailant through a display and/or speakers on the user's computing device. For example, the Responder may indicate, through the output subsystem of the user's computing device, to an assailant that they are being videotaped, that they should stop, or even that they are under arrest/being detained.

[0080] Dispatch Further Help (312). The Responder(s) may, through their computing devices/systems, dispatch additional support, such as emergency personnel or others to the location of the user as determined by their location information, which may be transmitted as coordinates or a map.

[0081] Store Incident Information (314). The information from the incident that is captured/obtained by the computing device of the user, such as all video, audio, locations, times, photos or other information may be stored, for example to apprehend or convict an assailant, determine fault, or aid in emergency medical diagnosis. Such information can be transmitted to one or more appropriate remote computer systems that can provide secure storage of the information (e.g., the data storage system 106).

[0082] Identification (316). In the case of an assailant, criminal, or other person, location or item involved in the incident, information captured/obtained by the user's

computing device may be used to identify that person, location or item. For example, an image of the assailant may be compared with photo or other databases to identify who the assailant is to aid in the later capture of the assailant.

[0083] Rewards/Incentives for Finding, Capturing (318). This system, which may be publicly accessible or otherwise accessible to a people who may be interested in/able to provide assistance (e.g., friends of the user, law enforcement), may be used to provide information or incentives to support others in supporting the user (including finding the user), or in capturing an assailant or other criminal involved in the incident.

[0084] Black Box Tracking (320). This system may be used to provide information about the user's situation at a later time that has been transmitted to a remote location, such as the user's locations, battery levels, photos, audio, video recorded from the device, calls, texts, other activities that may be helpful in determining if the user is safe or in danger, and their location. This allows the system to track things other than people as well, including vehicles, pieces of equipment, cargo, perishables, medical supplies, remotely or autonomously controlled vehicles including automobiles and flying drones.

[0085] FIG. 4 is a flowchart of an example technique 400 for initiating contact between a user's device and a responder. The example technique 400 is depicted as being performed in part by a user device 402, a responder device 404, and a computer server system 406.

[0086] The example technique 400 can be performed as part of technique 300, for example, at step 302.

Initiating a session and finding a responder to connect to

[0087] One type of example use case of steps depicted in figure 4 is that the user of a device may launch a safety application on their mobile device, their location, subscription level, and responder groups may be determined, and based upon this an available responder may be selected that is most appropriate for them (for example the responder in their primary responder group who is physically closest to them, available online, and in the correct jurisdiction). Then, a connection may be established with that responder, either for 'Ready Mode' or for initiating a two-way communication session.

[0088] The user device 402 may be any of a variety of appropriate computing device, such as a mobile computing device (e.g., mobile computing device 102, mobile computing device 202). For example, the user device 402 can be a user's IPHONE running an IOS app that allows user to press a button to initiate contact via any of a variety of appropriate connection, such as WiFi, BLUETOOTH, 3G/4G, other mobile or VOIP signal to contact a responder. In another example, the user device 402 can be a user's ANDROID device running an ANDROID app that allows user to press a button to initiate contact via any of a variety of appropriate connection,

such as WiFi, Bluetooth, 3G/4G, other mobile or VOIP signal to contact a responder. In a further example, the user device 402 can be a user's computer or tablet running an application that allows user to press a button to initiate contact via any of a variety of appropriate connection, such as WiFi, Bluetooth, 3G/4G, other mobile or VOIP signal to contact a responder.

[0089] The responder device 404 can be any of a variety of appropriate computing device (e.g., other computing devices 108a-d, other computing device 204), and can be similar to the user device 402. For example, the responder device 404 can be an IPHONE, an ANDROID device, a computer, or a tablet. Like the user device 402, the responder device 404 can also run an application, designed for an appropriate operating system of the responder device 404, to initiate contact over any of a variety of appropriate connections, such as WIFI, Bluetooth, 3G/4G, other mobile or VOIP signal to contact a responder.

[0090] The computer server system 406 can be any of a variety of appropriate computing device or devices that act in a server role providing information to clients in response to requests. For example, the computer server system 406 can be an application server that provides information for an application to client devices, such as the user device 402 and the responder device 404.

[0091] The user device 402 can launch the application (408) in response to any of a variety of appropriate inputs. For example, the application may be launched on the user device 402 by a dedicated or selectable/configurable button. The application may be launched on the user device 402 by pressing a virtual button on the device screen. The application may be launched on the user device 402 by dropping or shaking the device. The application may be launched on the user device 402 remotely by someone else, such as by a user of the responder device 404. The application may be launched on the user device 402 by voice command / voice recognition. The application may be launched on the user device 402 by automatic recognition of a surrounding event or situation (e.g., face recognition, location recognition, position recognition, proximity to another device or user, distance from another device or user, entering or leaving a defined area). The application may be launched on the user device 402, which may serve a role as a primary mobile device, by communication with another associated mobile device, such as a button on a watch, necklace, or other device. This other device may communicate with the primary mobile device by wired or radio communication, such as WiFi or BLUETOOTH.

[0092] In some implementations, after the application has been launched the application can enter Ready Mode (410). Ready Mode is a mode of operation during which connections with other computing devices, such as the responder device 404, are established and available in advance of initiating contact to communicate (e.g., video chat, call) with users of the other computing devices. The connections with the other devices can be peer-

to-peer connections. Ready Mode may be entered automatically after the application has been launched or may be entered in response to user input (e.g., selection of a physical or virtual button, shaking the device) directing the application to enter Ready Mode.

[0093] Ready Mode can be initiated on the user device 402 through the following steps 411-422. Steps 411a-d can be performed to identify appropriate devices for the user device 402 to connect with as part of Ready Mode. For example, some responders may need to be licensed within the jurisdiction (e.g., city, county, state, country) where the user device 402 is located to provide assistance to the user. Accordingly, the user device 402 can determine one or more jurisdictions that is currently located within and can identify licensure requirements for such jurisdictions (411a). Such jurisdictional determination may be done through local data sources, such as jurisdictional and licensing information downloaded and maintained on the user device 402, and/or through remote data sources, such as jurisdictional and licensing information maintained and made available by the server system 406 and/or other computer systems. In another example, the user may have a predefined list of other users, such as friends, family, and/or specific emergency responders, that the user prefers to use as responders. The user device 402 can request a group of responders that are included on the user's predefined list(s) and/or responders who are licensed to assist within the user's current jurisdiction (411b). Such a request can be provided to one or more remote computer systems, such as the server system 406 and/or other computer systems.

[0094] Using the initial group of responders who satisfy one or more criteria (e.g., on the user's predefined list, able to assist within the jurisdiction) for the user device 402, the user device 402 can determine which of those responders are currently available to assist (411c). Such a determination can be made by polling the responder devices and/or by polling a remote computer system (e.g., server system 406) that maintains status information (e.g., current availability) for the responders. From the identified responders (e.g., available responders able to assist within the jurisdiction), the closest responders can be determined (411d). Such a determination can be made by obtaining location information for the responders, determining distances from their locations to the location of the user device 402, and identifying a portions of the responders who are closest to the user device 402 (e.g., closest n responders, responders within threshold distance). The location information for the responders can be obtained by polling the responders and/or by requesting such information from a remote computer system (e.g., the server system 406). The steps 411a-d, in whole or in part, may alternatively be performed by a remote computing device, such as the server system 406, and/or may be performed in association with different steps in the technique 400, such as being performed at step 430.

[0095] To establish a peer-to-peer connection with the

responder device 404 as part of Ready Mode, the user device 402 can transmit a request for the network addresses (e.g., IP addresses, local area network addresses) other computing devices associated with responders (412), such as the responder device 404. The request can be transmitted to the server system 406, which can maintain a list of the current network addresses (e.g., IP addresses) of computing devices that are using the application and services provided by the server system 406. The request can include information identifying the user device 402 and/or a user of the user device 402, such as a user id.

[0096] The server system 406 can receive the request (414) and can identify network addresses for other computing devices (416). The server system 406 may limit the network addresses that are identified to particular other computing devices, such as those that have been preselected by the user of the user device 402 as responder (e.g., family, friends), responders that are located near the user device's current location (e.g., police officers located near the user device 402, an appropriate 911 dispatch given the location of the user device 402, other users who are located with a threshold distance of the user device 402), and/or responder services (e.g., professional security services) that can manage response efforts and that can involve additional responders, such as police and other emergency responders, as needed. Once identified, the server system 406 can transmit the IP addresses to the user device 402 (418).

[0097] The user device 402 can receive the IP addresses (420) and can use them to establish Ready Mode connections with responder devices, such as the responder device 404 (422). The responder device 404 can connect with the user device 402 (424). The connection between the user device 402 and the responder device 404 can be peer-to-peer, which may be blocked by firewalls at either end of the connection. To avoid this a variety of techniques can be used, such as both sides attempting to connect to each other simultaneously (in case one side can't accept incoming connections but can make outbound connections), hole punching (e.g., UDP hole punching, TCP hole punching), and/or deploying relays (e.g., TURN servers).

[0098] The user device 402 can display (or otherwise present) the responders who are connected to the user device 402 in Ready Mode. Examples of such a display are depicted in Figures 10-11. In Ready Mode, a peer-to-peer connection is established between the user device 402 and the responder device 404, as indicated by steps 422 and 424. Thereafter, in Ready Mode the user device 402 can display the Responder continuously by live video, or may display an image of the available responder, with such video and images being transmitted from the responder device 404 to the user device 402 over the established peer-to-peer connection. This allows the user to see that the responder is available. The responder device 404 may not receive videos or images from the user device 402 and, thus, the responder may

not see the user. The responder device 404 can be available to many users at once in this mode. In some implementations, the responder device 404 may receive and display the plurality of users connected to the responder in Ready Mode by live video. In some implementations, the responder device 404 can see the plurality of users connected to the responder in Ready Mode by live video while the user devices (e.g., user device 402) do not receive or display video or images of the responder.

[0099] Whether or not in Ready Mode (the user device 402 does not need to first enter Ready Mode), the user device 402 can monitor for user input to initiate contact with one or more responders. When the user device 402 receives input to initiate contact with a responder (430), who may or may not be specified through the input, the user device 402 can select one or more responders to which the contact should be initiated (430) and can proceed to initiate contact with the selected responders (432), which can be accepted, automatically or in response to user consent, by the responder device 404 (434). The contact can include communication with a responder, such as video conferencing, audio conferencing (e.g., telephone call), and/or text messaging.

[0100] Contact can be initiated in a number of ways, such as shaking and/or dropping the user device 402 (e.g., detected through measurements by accelerometer(s)) and/or releasing contact with a virtual and/or physical button to indicate an emergency or intent to initiate contact. For example, in Ready Mode, a user may press a button (or provide input in any other appropriate way) to initiate contact with the Responder. Since the connection, which may be a peer-to-peer connection, between the user device 402 and the responder device 404 is already made through Ready Mode, a live video or audio call may be started between the user device 402 and the responder device 404 substantially immediately, for example in a fraction of a second.

[0101] Responders can be selected for contact at step 430 in any of a variety of ways. For example, any available responders can be selected for contact with the user device 402. In another example, responders can be selected based on the location of the user device 402 and the responders. For instance, contact may be initiated with the nearest available responder based upon the localization information of the responder and user device 402, which can be provided for in any of a variety of ways, such as by GPS, WiFi, cellular, or pre-defined localization information (E.g. physical address). In another example, responders can additionally be selected based on preferred responder lists that have been designated by the user of the user device 402, such as lists identifying particular family members or friends. Such lists may provide cascading lists of preferences and/or may designate particular responders for particular situations (e.g., medical emergency, crime). Other responder lists may also be used, such as dedicated lists of emergency responders that service an area where the user is located. In a further example, responders can additionally be selected based

on user ratings of responders. For instance, responders who have been rated as providing great service may be preferred and selected over other responders who have been rated as providing poor levels of service.

[0102] The contact can be made using any of a variety of appropriate protocols, such as peer-to-peer ad-hoc networks for audio or video or data communication, communication with or through a central server (e.g., the server system 406), and/or wireless communication using existing or future protocols, such as chat protocols (e.g., open system for communication in realtime protocol (OSCAR), talk to OSCAR protocol (TOC), iMessage protocol, Gadu-Gadu protocol, simple anonymous messaging protocol (SAM), ICQ protocol, internet relay chat protocol (IRC), QQ protocol, secure internet live conferencing protocol (SILC), Skype protocol, extensible messaging and presence protocol (XMPP), Microsoft notification protocol (MSNP), web real-time communication protocol (WebRTC)), voice over IP (VoIP) and video conferencing protocols (e.g., H.323, Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP), H.248 (also known as Media Gateway Control (Megaco)), Real-time Transport Protocol (RTP), Real-time Transport Control Protocol (RTCP), Secure Real-time Transport Protocol (SRTP), Session Description Protocol (SDP), Inter-Asterisk exchange (IAX), Jingle XMPP VoIP extensions, Skype protocol, Teamspeak), messaging protocols (e.g., short messaging service (SMS), multimedia messaging service (MMS), enhanced messaging service (EMS)), and/or other appropriate communication protocols.

[0103] Contact and other functionality described here may use existing or future one-to-many, many-to-one and many-to-many connection systems, including social networks, such as FACEBOOK, TWITTER, SNAPCHAT, INSTAGRAM, WHATSAPP, VINE, email, and/or other appropriate systems.

[0104] The state of the user, friend or responder may be viewable by their peers/friends/opponent, including but not limited to whether the person is in the app (e.g., has launched the application, is currently using the application, whether the application currently has focus on the user's device), whether they are already on the phone or on a video call or participating in text messaging, when the last time that they communicated was, what their last location was, whether they are at a designated location, and/or whether they are currently located in a safe or dangerous or other zone (e.g., using pre-defined 'geofenced' areas defined geographically or by proximity to a given location).

[0105] As part of the contact and communication between the user device 402 and the responder device 404, the user may record video of themselves or their surroundings using a plurality of cameras on their mobile device (user device 402), as depicted in FIG. 10-11. Some of the features that may be included in this mode are shown in these figures. This video may be saved locally on the user's device, may be saved to the responder's device, or may be saved to the web/internet/cloud

on a filesaver.

[0106] FIGS. 5A-F are flowcharts of an example technique 500 for communicating between a user device and a responder device as part of a security session. The example technique 500 can be performed in part by the example user device 402, the example responder device 404, an example data storage system 403, an example restricted computer system 405, example other responder devices 407, an example emergency responder device 409, and example other devices 411. The example data storage system 403 is a computer system that remotely stores data transmitted by user and responder devices, and can be similar to the data storage system 106 and/or the data storage system 208. The example restricted computer system 405 can be a computer system that restricts data access to particular authorized users, such as computer systems associated with law enforcement (e.g., local police, FBI, CIA), the military (e.g., DOD, army, navy, airforce, marines), social networks (e.g., FACEBOOK, TWITTER), and/or other private companies (e.g., security companies, data aggregators). The example other responder devices 407 can be devices that are associated with additional responders who are different from the responder device 404. The example emergency responder device 409 can be associated with one or more emergency responders (e.g., police, fire fighters, EMTs) and can be a handled computing device (e.g., smartphone) or an embedded system within a mobile unit (e.g., car, ambulance). The example other devices 411 can be other computing devices that are available for receiving and outputting audio/visual information.

[0107] FIG. 5A depicts two-way communication between the user device 402 and the responder device 404, while concurrently securely transmitting and storing data associated with the communication at the data storage system 403. For example, FIG. 5A depicts steps for continuous real time recording and transmission of information from the user device 402, continuous real time recording and transmission of information from the responder 404, and helping the user of the user device 402, as described above with regard to steps 304, 306, and 312, respectively.

Connection, Location, Secure Two-Way Communication, Transmission and Storage of Data

[0108] Information from the user device 402 or their situation may be transmitted in substantially real time to the responder 404 (or multiple responders). This information from may include audio/video from the user's device, photos, GPS or other localization information. All of this information may be transmitted synchronously or asynchronously (with a delay). The intent may be to ensure that as much information is transmitted as possible, especially in the event that the time to transmit is limited. This information from may include audio/video from the user's device, photos, GPS or other localization information.

[0109] For example, the user device 402 determines its location (501) (e.g., determining GPS coordinates, determining micro-location), records audio and video using microphones and cameras that are part of or accessible to the user device 402 (502), obtains sensor data from one or more sensors that are part of or accessible to the user device 402 (503) (e.g., time sequenced motion sensor data), accesses data from one or more devices that are connected to the user device 402 (504) (e.g., obtain audio and/or video signals from wearable devices with cameras and/or microphones, obtain motion sensor data), and packages the obtained data (location, audio/video, sensor data, other data) for secured and verified transmission to the responder device 404 and, concurrently, to the data storage system 403 (505).

[0110] The video can be obtained by the user device 402 using equipment capable of detecting electromagnetic radiation outside of the visible spectrum, such as infrared signal and/or other night vision technologies. Additionally, the user device 402 may include technology that is capable of detecting the presence and location of nearby physical objects, such as through sonar devices and other appropriate technologies. Depending on the situation facing the user, it may be difficult for the user to maintain a steady camera shot. The user device 402 can use image stabilization technology, both hardware and software, to produce video that will be easier for the responder to view and understand. Additionally, the user device 402 can passively obtain information regarding other devices that are located nearby that are transmitting wireless signals which may provide a lead as to the identity of the assailant. All such data, and other data not explicitly described but available or accessible to the user device 402, can be obtained, packaged, and transmitted to the responder device 404 and the data storage system 403.

[0111] The packaging of the data may be provided using means that allows for verification of a secure and validated connection or transmission path from the user to the recipient, or to online storage. For example, information transmitted between the user and responder, or recorded by the user or responder, may be encrypted using digital encryption, and may also include a custom digital watermark or timestamp or location stamp that may also use encryption to verify the identity and time of transmission of the user, responder or both. This technology may provide a means of verification of information transmission, for example for the use in verifying from when and where and what user this information was transmitted. This may be used later to verify this information for use as evidence. These encryption steps may be performed locally on the mobile device of the user. These encryption steps may be performed on the responder device. These encryption steps may be performed on a remote server.

[0112] The user device 402 can transmit the packaged data to the responder device 404 and to the data storage system 403 (506). The responder device 404 can update

the presentation of information about the user based on the received data, such as displaying the received user video, audio, and data (511) and updating a display of the current location of the user device 402 (512). Additionally, the responder device 404 can store the data received from the user device 402 as well as the data obtained on and transmitted by the responder device 404 (513).

[0113] The responder device 404 can obtain and transmit similar information to what the user device 402 obtained and transmitted, which may be transmitted in substantially real time to the user device 402. This information may include audio/video from the responder's device, photos, GPS or other localization information. For example, the responder may be displayed on the user's device, as in videoconferencing, video chat, and/or video broadcast. Also, pre-recorded audio, images, or video may be transmitted by the responder device 404 and displayed on user device 402.

[0114] For example, the responder device 404 can determine its location (507), record video and audio of the responder using cameras and microphones that are part of or connected to the responder device 404 (508), and package the data for secure and verified transmission in the same way as the packaging of the user device data (509). The responder device 404 can transmit the packaged data to the user device 402 and the data storage system 403 (510).

[0115] The user device 402 can display the video and audio of the responder (514) and update a display of the responder location, such as on a map that is displayed in conjunction with the video of the responder (516). In addition to storage by the responder device 404, the user device 402 can store the data received from the responder 404 and the data obtained and transmitted by the user device 402 (516). The video and audio of the responder that is output by user device 403 can help the user, for example by communicating with the user and/or with a potential assailant. For example, the Responder may indicate to an assailant that they are being videotaped, or even that they are under arrest/being detained. In some implementations, the user device 402 the user and responder data can be stored on the user device 402 and/or the responder device 404, and uploaded to the data storage system 403 at a later time, such as when a reliable network connection with the data storage system 403 can be established.

[0116] Concurrently with the recording, transmission, and output of real-time information between the user device 402 and the responder device 404, the data storage device 403 can receive and store incident information pertaining to the communication between the user device 402 and the responder device 404. The information from the incident, such as all video, audio, locations, times, photos or other information may be stored, for example to apprehend or convict an assailant, determine fault, or aid in emergency medical diagnosis. As indicated by step 516, this information may be stored on the user's device

402. As indicated by step 513, the information may be stored on the responder(s) device 404. The information may be stored to a central database on a central server, such as the data storage system 403.

[0117] For example, the data storage system 403 can receive the responder data (517) and the user data (519), and can trace the routes over which the responder data and user data are received so as to provide evidence of the chain of transmission (518, 520). The received data and any verification information that is determined or obtained, such as trace routes and timestamps, can be securely stored by the data storage system 403 (521). Such secure storage can include encryption, such as encryption performed by the user device 402 and/or the responder device 404, and/or encryption performed on the data by the data storage system 403.

[0118] The information that is stored by the data storage system 403 may be made available later to the user, their supporters/contacts, to emergency personnel, to the general public, or to others. Real time reports of the nature and location of incidents, and any other information provided by this system may be provided to those who need it. In some implementations, emergency responders or police officers carrying mobile devices running the software provided for here may receive real time alerts when an event has taken place near them, including mapped information of its location, photo, video, audio or other information collected about the event. The responders contacted may include those closest to the site of the incident. In some implementations, users of this system may receive real time alerts of nearby incidents, or a map of incidents in their vicinity, which may be sorted or filtered by the time when the event occurred, proximity, types of event, or other factors.

[0119] The described storage, transmission and other functions may be performed with or without encryption of the information. All of the information may be owned, controlled, or password protected by the user, emergency responder, provider of this technology or others. All of the information collected by this technology may be provided in substantially real time via the web, for example provided to the user, a friend of the user, the responder, or a court. All of the information collected by this technology may be saved, and provided later via the web, for example provided to the user, a friend of the user, the responder, or a court. The control over the dissemination of this information may be given to the user.

[0120] As indicated by the arrows looping back to step 501 from step 516, to step 507 from step 513, and to 517 from step 521, the transmission, display, and storage of information across the user device 402, the responder device 404, and the data storage system 403 can be continuous during the 2-way communication between the user and the responder.

[0121] Although described as being performed in association with the two-way communication, the storage of data from the user device 402 and/or the responder device 404 at the data storage system 403 may be per-

formed independent of the communication. For example, the user device 402 may begin transmitting data (e.g., location, video, audio, sensor data, peripheral device data) to the data storage system 403 for storage without being involved in a communication session with a responder device.

[0122] Screenshots are shown in FIGS. 11A-E, and described in greater detail below, show example screens that can be displayed to the caller (user device 402) and a responder (responder device 404) during 2-way communication sessions.

[0123] The responder device 404 can additionally perform a variety of actions in association with and during the 2-way communication with the user device 402. Such action, which are linked to by the circles A-E, can be performed alone or in any variety of combination with each other and are described with regard to FIGS. 5B-F.

[0124] For example, the responder or user may use pinch-to-zoom video on their own video or the opponent's (peer's) video. The responder or user may see a pinch-to-zoom or other map of the opponent's location, or may receive their address. The Responder may have an automatic or one-click way, through the responder device 404, of connecting with emergency responders responsible for the user, such as connecting with the closest or most appropriate 911 or emergency dispatch center to the user device 402 (e.g., using a PSAP dip procedure). This feature may also allow transmission of information to the 911 or emergency dispatch center, including all aspects of the information/communication between the responder device 404 and user device 402, including but not limited to the user's name, id, photo, video, audio, geolocation, situation, etc. The user's mapped location may be updated on the responder's device 404 in substantially real time, and may be presented to the responder using coordinates (including lat/long/elevation or others), an address or other place location identifier, the location of a previously-identified location such as home, school or a business name, or by depicting the user's name, userid or image on a map, which may be a pinch-to-zoom map.

[0125] FIG. 5B is a flowchart that depicts steps 522-530 for remote control of one or more features of the user device 402 by the responder device 404. For example, the responder, through the responder device 404, may remotely control the features of the users device 402, for example to take high resolution photos and have them sent, pan, focus, zoom, crop video/camera, capture audio, adjust volume, turn on/off speaker or speakerphone, turn on/off lights, turn on/off alarms, initiate contact with other users, responders, or emergency services (e.g. 911 or other emergency services call) from the user's device 402.

Remote Control

[0126] An example use case is that a user may want to start audiovisual two-way communication with the mo-

bile device of their friend (if their friend has given them permission to do so), without the friend having to interact with the friend's device. This may be useful in situations where the friend may not be able to interact with their device, for example if they are not in possession of it, or if they are restrained or incapacitated in some way. Another example use can be that a user may want to start audiovisual two-way communication with their own mobile device, for example if their device is lost, so that they can see what is near their device to try to recognize its location, or communicate with anyone nearby, or send a pre-recorded message, such as explaining the owner of the device or giving instructions to anyone who can hear.

[0127] The responder device 404 can receive input to control one or more features of the user device 402 (522). Based on the received input, the responder device 404 can obtain additional information to be output with the controlled feature on the responder device 402 (523). For example, the responder can select an audio recording to play on the user device 402 (e.g., siren, message warning assailant to leave the user alone). In another example, the responder can select an image to present on a display of the user device 402, such as zoomed in and enhanced image of the assailant's face so as to demonstrate to the assailant that their identity has been recorded by a third party monitoring the situation. The responder device 404 can transmit the control instructions and additional information to the user device 402 (524).

[0128] The user device 402 can receive the instructions and additional information (525) and can check permissions to determine whether to perform the operations instructed by the responder device 404 (526). The permissions may be predefined and/or rule based, and may be explicitly identified (e.g., preapproved list of responders with permission) or implicit (e.g., any responder that was contacted by the user device 402 can be provided with implicit permission). If the responder device 404 is determined to have permission, the user device 402 can proceed to execute the instructions (527). For example, executing the instructions may toggle various feature on/off, such as cameras, speakers, microphones, displays, and/or lights (flashlights), and/or allow various adjustments to be made to currently enabled features, such as allowing for pin and zoom of the camera on the user's device 402 by the responder device 404. If additional information is provided by the responder device 404, it can be output by the user device 402 (528) (e.g., display image and/or play an audio file provided by the responder device 404). The user device 402 can report the status of the instructions (e.g., status of the feature that was changed) to the responder device 404 (529), which can in turn display the status information to the responder (530).

[0129] FIG. 5C is a flowchart that depicts example steps 531-541 for identifying an assailant based on information received from the user device 402. In the case of an assailant, criminal, or other person, location or item involved in the incident, information obtained by the user

device 402 may be used to identify that person, location or item.

Identifying a Person or Assailant

[0130] In an example use case, photos or video of an assailant, user, or other person, landmark or object may be compared with photo or other databases to identify who/what they are. In the case of an assailant, this may be used for later capture, or this identity information or other information about the identified person may be transmitted to the user in substantially real time.

[0131] For example, information collected from the user device 402 about an assailant or other criminal suspect may be compared manually or using automatic image-recognition software against databases of images of people, including past-criminal databases, to identify the likely identity of suspects. This approach may be used with other types of information, including audio recordings (voice pattern matching), gate and movement information, other biometric information. This information may be used in combination other information to improve accuracy. Such other information may include locations, affiliations, types of prior crimes, or other information to narrow down searches.

[0132] The responder device 404 can initiate identification of an assailant, objects, and/or a location where the user device 402 is located either automatically upon receiving data from the user device 402 or in response to input from the responder to begin such a process (531). The responder device 404 can identify features (e.g., face, proportions, size, shapes) of the unknown assailant, object/location from the data received from the user device 402, such as photos, videos, audio data, and/or nearby wireless devices (532). The responder device 402 can perform one or more identity matching operations for such features using local data sources, such as data sources that are maintained by the responder device 404 (e.g., repository of user identities) (533). The responder device 404 may additionally draw on data sources that are maintained by one or more restricted computer systems 405, such as computer system maintained by police, military, social networks, and/or private companies (534). Such other data sources can include a variety of identifying information on users, such as images, voice patterns, recent/current location information, and/or proportion information.

[0133] For example, in addition to having user profile information (e.g., name, address, telephone number, registered vehicles) the entity associated with the restricted computer system 405 may obtain consent from users to receive and use current location information for the users. For instance, car insurance companies offer the possibility of discounts to their customers in exchange for constantly tracking the location of their car. In another example, users frequently offer their location information to social networks as a way of notifying others of their location and/or receiving rewards. Government entities

track the location of criminals through the use of monitoring bracelets, which can be offered and used as a way for released criminals to prove that they were not involved in a new crime for which they may be suspect based on their time sequenced location data. The restricted computer system 405 can obtain such user location updates (536) and can accordingly update its database (537), which the responder device 404 can be provided with access to (535) to perform its identity matching.

[0134] Based on the identity matching, the responder device 404 can determine one or more candidate identities for the assailant/object/location (538), which can be transmitted to the user device 402 (539) and stored locally on the responder device 404 (541). The user device 402 can receive the identity information and can present/display it to the user and/or assailant (540). For example, the user device 402 can receive the identity of the assailant and can announce the name of the identified assailant as well as the assailant's address and telephone number. Such information can be persuasive in convincing an assailant that they are not going to get away with a crime against the user if one is perpetrated, and can accordingly act as a deterrent from such action and provide security to the user.

[0135] FIG. 5D is a flowchart that depicts example steps 542-550 for remotely helping the user device 402 initiate and establish a connection with another device 407.

Initiating Communication Between Other Parties

[0136] In an example use case, the responder device 404 can make a communication connection between the user device 402 and a safety responder's device (example other device 407), so that communication begins between the user and the safety responder. This communication connection may include an audio call, video call, instant messaging session. All of these may take place within a dedicated app, or may take place using standard infrastructure (e.g. third party phone lines, SMS connection, videoconferencing capability). For example, if person A receives an alert message that their friend person B may be in trouble, person A can directly initiate communication between person B and safety responder R, including without person B or responder R performing any additional action.

[0137] In another example, the responder device 404 can make a communication connection between the user device 402 and a device (other device 407) of one of the user's friends, so that communication begins between the user of user device 402 and the friend of that user. This may take place even though the responder may not have direct knowledge of who the friend of the user that they are forming the connection to is. For example, the responder may send out a message or connection request to all of the friends who the user of user device 402 has previously selected, even though the user of user device 402 may not have direct access or knowledge of

this list. This communication connection may include an audio call, video call, instant messaging session. All of these may take place within a dedicated app, or may take place using standard infrastructure (e.g. third party phone lines, SMS connection, videoconferencing capability).

[0138] In another example, the responder 404 can perform any of the other functions provided here on the user device 402. Some of these include: reporting an incident, taking a photo, uploading text, a photo, audio or video to the cloud (including using encryption based on the user device 402's encryption information, the responder device 404's encryption information, or both), placing a text message from the responder device 404 to authorities (e.g. to a PSAP/911 dispatch center), connecting with one of the responder's hero (designated/preferred responders), even if the user of user device 402 does not know who this is.

[0139] The responder device 404 can receive input suggesting that the user may need help or requesting that the user device 402 connect with the other device 407, even though the identity of the other device 407 and/or a user of the other device 407 may not be known to the responder or the user of the user device 402 (542). The responder device 404 can transmit control instructions to initiate the connection to the user device 402 (543).

[0140] The user device 402 can receive the control instructions (544) and can check whether the responder device 404 is permitted to perform such an action (545). The permissions may be predefined and/or rule based, and may be explicitly identified (e.g., preapproved list of responders with permission) or implicit (e.g., any responder that was contacted by the user device 402 can be provided with implicit permission). If the responder device 404 is determined to have permission, the user device 402 can proceed to initiate the connection with the other device (546). If the identity of the other device is not specified in the instructions from the responder device 404, the user device 402 may proceed to select an appropriate responder, similar to the techniques described above with regard to step 430 in FIG. 4. If the IP address of the other device 407 is not known, the user device 402 can automatically identify it by contacting a central server system 406, as described with regard to steps 412-420.

[0141] The other device 407 can accept the connection with the user device 402 (547) and communication between the other device 407 and the user 402 can take place, which may additionally include communication with the responder device 404 (548-550).

[0142] Of the steps 542-550 that are described as being performed by the responder device 404 can also be performed in the reverse by the user device 402, and vice versa.

[0143] FIG. 5E is a flowchart that depicts example steps 551-560 for routing the user device 402 to an appropriate emergency responder 409.

Routing Connection to An Appropriate Responder

[0144] In an example use case, identifying an appropriate emergency responder to handle a particular type of incident at a particular geographic location can be a complex issue to solve, especially when the user requesting services is not automatically routed through a public system (PSTN) to an appropriate local responder. For instance, the jurisdictions for different types of emergency responders (police, fire fighters, EMS) may not correspond to each other and may change frequently, even depending on the current day and time.

[0145] To properly handle and route the user device 402 to the appropriate emergency responder 409, the responder device 404 can access user profile information for a user of the user device 402 (551). Such information may be stored locally by the responder device 404, which can be a part of a professional security service with which the user of the user device 402 has established an account. Accordingly, this may save the user from having to provide all of his/her pertinent details (e.g., name, age, address, medical conditions, appearance, contact information) and, instead, the user device 402 may simply provide his/her id (e.g., device id, user id) with the responder device 404 for retrieval of this information.

[0146] The responder device 404 can access emergency routing information, which may be maintained in an up-to-date state by the responder device 404 (552), or in a connected network or database. Such emergency routing information can include geographic boundaries for various emergency responders, rules for when these boundaries may change, and other nuanced information regarding coverage by emergency responders in various geographic locations. An example of such emergency routing information is a PSAP system. In this example, the responder may determine the correct 911 or emergency dispatch center (or PSAP) based on the physical location of the user.

[0147] The responder device 404 may additionally have access to information regarding emergency responders and their current status (e.g., working, on a call, available, offline). Such access may be limited to particular responders, such as professional security service providers which may have contracted with various emergency responders throughout a geographic region to have access to such information. The responder device 404 can access the emergency responder information (e.g., skills, training, experience, geographic locations served, previous results) and the current status information for the emergency responders (554). The emergency responders for whom this information is obtained may have been selected based on the appropriate emergency routing information.

[0148] A portion of the emergency responders that are identified and for whom status information has been obtained can be selected based on a variety of factors, such as current availability, proximity to the user of the user device 402, appropriate training, skills, and/or experi-

ence to handle the user's situation (555), and the user's membership in different responder groups, or the user's subscription status or level (for example free, paid, premium). With the appropriate emergency responder(s) selected, the responder device 404 can route information regarding the user and the incident to the emergency responder device 409 that is associated with the selected responder (555).

[0149] The emergency responder 409 can receive the information regarding the user and the incident, and can use that information to begin providing assistance to the user (556). Such assistance can include travelling to the user's location or dispatching someone to the user's location (as conveyed in the information from the responder device 404), monitoring the user's situation (can be linked to the responder's data feed from the user), and/or can initiate contact with the user device 402 (559). The user device 402 can accept such contact 560, for example, the user device 402 may auto-answer the contact request from the emergency responder 409 and/or permit access to control of features on the user's device 402 (560).

[0150] For instance, the responder device 404 may dispatch additional support, such as emergency personnel or others to the location of the user device 402 as determined by their location information, which may be transmitted as coordinates or a map. For example, the responder(s) or contacts of the user may receive a map with real time updates showing the user's location, and/or their location, and/or the location of other responder(s) or contacts involved or potentially involved in supporting the user in their situation. This may include either the pre-selected contacts of the user, or other people available for support, such as other members of a network of people using this technology who have offered to be of service.

[0151] The responder device 404 may also notify the user of the selected emergency responder 409 (557), which the user device 402 can display to the user or others nearby (558).

[0152] FIG. 5F is a flowchart that depicts example steps 561-571 for causing other devices 411 that are located near the user device 402 to audibly and/or visually output information or record or monitor information.

Engaging Nearby Devices

[0153] In an example use case, the responder device 404 can direct the other device 411 (e.g., devices with displays and speakers) to output alarms and other messages (e.g., audio and/or video recorded of the responder) to solicit help for the user of the user device 402 from people located nearby and/or to identify the assailant to others in the area. For example, if a user is in an emergency in a public or private facility with appropriate other devices 411, they can activate emergency alarm sounds or lights or recording on the other devices to enhance their safety, or the safety of others at the facility.

[0154] The responder device 404 can receive input to request information regarding devices that are located nearby the user device 402 (561). The responder device 440 can transmit the request to the user device 402 (562), which can receive the request (563) and identify nearby devices through polling the devices (564). Polling of the devices can be performed on a periodic and/or continuous basis, and can be performed before the input to request information about nearby devices is received. The other devices 411 can transmit their identities (565), which can be detected by the user device 402. The user device 402 can transmit information (e.g., existence, identity, type of device) regarding the nearby device to the responder device 404 (566), which can display information regarding the nearby devices to the responder (567a). The information can additionally be stored (e.g., by the responder device 404 or other computer devices, such as the data storage system 403) (567b) and access can be provided to it as a form of evidence of what is/has happened to the user of the user device 402 (567c). The responder device 404 can receive instructions to output particular information on one or more of the nearby devices (568), which can be transmitted to the user device 402 (569).

[0155] The user device 402 can receive the instructions (570) and can transmit the instructions with the particular information to the nearby devices (571). The other devices 411 can receive and output the particular information (572).

[0156] The example technique 500 can be used in a variety of scenarios. For instance, in one example medical emergency scenario the user has a medical emergency, uses their mobile device (user device 402) to run an app provided for by the disclosed technology to connect a video session with a responder (responder device 404), and the responder may communicate with the user, view the user or their emergency situation, offer advice, dispatch medical care or other personnel, or contact others.

[0157] Assailant Scenario In an example assailant scenario, the user is attacked or threatened by an assailant. The user may deploy their mobile device (user device 402) to dissuade such an assailant. If the user holds up the device 402, the disclosed technology provides that the device 402 and software may take video recordings of the assailant, and may allow the assailant to see a police officer, security officer, emergency responder, or one of the user's contacts, who may communicate with the assailant. For example, the responder (using responder device 404) may say "I see you, I have recorded images and video of you, we can identify you, we know exactly where you are, and anything further that you do may be used against you in a court of law." If the responder is a police officer, they may even place the assailant under arrest or detain them until law enforcement arrives on the scene, and the responder may further indicate that running away would be resisting arrest. The app/device (user device 402, responder device 404) may also send

out an emergency alert to emergency services (e.g. US 911), and may send out alerts to pre-selected contacts by any means, including SMS, email, push notification, call, satellite link, pager network, videochat or others.

[0158] Lost User Scenario In an example lost user scenario, if a user is lost, the device (user device 402) may be useful in finding them. For example, if the user has been running an app provided for by the disclosed technology on their mobile device (user device 402) that periodically measures their location using GPS, cell-tower-based localization, wifi-based localization, or other localization technology, this information may be stored on the user's device 402, or it may be transmitted to a remote location where it is stored in a database (data storage system 403), allowing the user's last known location to be used to search for the user. In addition, if the user still has a connection, the user may use the app to initiate audio or video communication with one or more emergency responders, or with one or more of their contacts. Information may be transmitted about other aspects of the user's behavior that could indicate their status, such as their remaining battery, accelerometer data, when they last sent text messages or emails or made calls, or used their device (user device 402).

Suspicious Scenario

[0159] In an example suspicious or fearful scenario, if a user feels that they are in a suspicious or fearful scenario where they are concerned that they may be in danger, they may use this technology on their mobile device (user device 402) to record people or events in their vicinity, to signal to an emergency responder that they are concerned, to signal to their pre-selected contacts that they are concerned, and/or to provide information about their estimated location based on GPS, cell, WiFi, etc. as above. The device/software (user device 402) may also allow them to be in audio and/or video communication with a responder (responder device 404). The device/software (user device 402) may also allow them to automatically initiate contact after a pre-defined time if they have not cancelled. The device/software (user device 402) may also provide for them to hold down a button which, if released, initiates automatic contact or sends out an emergency signal to responders or contacts as provided for above.

Motor Vehicle Scenario

[0160] In an example motor vehicle recording scenario, this technology may be used in or around a moving vehicle to observe accidents or video record surroundings or other drivers, and this information may be logged in the device (user device 402) and/or transmitted to a remote network (data storage system 403). In the event of a user being in an accident, this information may be used in determining that an accident has occurred (accelerometer information may be particularly useful in

measuring their velocity/acceleration to determine that there was an accident), determining the user's location, determining the user's situation, and determining fault in an accident (e.g. using video of the user's vehicle and other vehicles). The device (user device 402) may be mounted to the users' dashboard, windshield, mirror, bumpers, roof, or other location chosen to facilitate recording. This information may be used to call remote assistance for the user, either automatically or by a human responder. This may be used in connection with any type of vehicle, including automobile, truck, military vehicle, boat, airplane, spacecraft, bicycle, train, bus, public transit, automatous vehicle. The device may also interface wirelessly or by wired connection with other onboard computers and sensors of the vehicle, including cameras, pressure sensors, temperature sensors, vibration sensors, electrical sensors and others and may transmit any of this information to a remote server (where it may be recorded), or a responder in communication with the user. This may be useful in determining the situation of the user in an emergency, assisting the user, or for later use as evidence.

[0161] FIG. 6 is a flowchart of an example technique 600 for facilitating auto-answer features between a user device 402 and a responder device 404.

Auto Answer or Auto Connect

[0162] For example, the technique 600 allows the responder device 404 (which may be associated with a user, emergency responder, professional security service) to place a call to the user device 402 in such a way that the user device 402 automatically answers the call, even without the user's further action. For example, the responder device 404 may place a videocall from the responder device 404 (e.g., mobile phone) to user device 402 (e.g., mobile phone). Without the user of the user device 402 taking any further action, the software on the user device 402 (e.g., phone) automatically accepts the connection from the responder device 404. This may provide that the responder device 404 can then see video input and audio input from user device 402 (e.g., phone). The responder device 404 can also transmit their own audio (e.g. speech) and video to user device 402. All of this may be recorded. This provides a means that in an emergency situation, where the user of the user device 402 may not have access to their phone, may be incapacitated, or may be unable to press a button on their phone, the responder device 404 may still initiate communication without requiring action by the user of the user device 402. In addition, this provides a means for remote control of a device that is located someplace where it is desirable to be able to automatically initiate one-way or two-way audio, video, communication, or the other aspects of this technology. For example, a device may be mounted to a wall, or inside of a vehicle, or inside of a home or business and may act as a remotely-controllable security camera. In addition, the device may

make it possible to communicate by audio and/or video to the remote location. For example, if the device is mounted to a wall as a security camera, in the event of an intrusion, the device can begin automatically recording (including using motion and sound detection), and can also automatically place a connection to a responder, and the responder can be displayed in substantially real-time on the screen of the device, control the device, and interact with any potential intruder through two-way audio and video. In this way, a security person at a remote location can remotely intervene to stop an intrusion or other crime or inappropriate action.

[0163] In workplace settings, this technology may allow for a responder to take control over a device and begin recording and two-way communication with anyone at the scene. Example use cases include the responder serving as a remote teacher or instructor, performing quality assurance or examining work, examining items at the scene such as to determine damage to items or to assess the quantity or quality of stock. This remote control technology may also be used for the responder to be involved in remote monitoring, assistance and training in a number of contexts, including repairs, medical procedures, conversations with patients, and conversations with people at the remote scene. All of this may be recorded securely to the remote server.

[0164] The responder device 404 obtains user device 402 status information, such as information indicating whether the user device is online, offline, currently being used, on a call, and/or has not been used for n minutes (602). Such status information may be obtained through communication with a central server system. The responder device 404 can additionally receive an indication as to whether the Responder has been provided auto-answer permissions for the user device 402 - meaning that the Responder is able to initiate and automatically establish calls on the user device 402 (604). Based on the indication, an auto-answer calling feature can either be activated or deactivated on the responder device 404 (606). For example, the auto-answer calling feature can be a virtual button on the responder device 404 that, when enabled, is presented and is responsive to user contact. In contrast, if the auto-answer calling feature is inactive, such a virtual button may not be displayed or may be otherwise indicated as being inactive (e.g., presented in gray/colorless manner).

[0165] The responder device 404 can receive selection of the auto-answer feature (608) and, in response to receiving the selection, can initiate auto-answer communication with the user device 402 (610). The communication can be one or two-way audio and/or visual communication. Auto-answer communication may be different from regular communication by the virtue of metadata that is transmitted indicating that it is an auto-answer communication request.

[0166] In response to receiving the request, the user device 402 can accept the auto-answer request (612) and can, without prompting the user of the user device

402 for consent first, obtain and transmit data (e.g., audio and/or video data, location data, device state data) to the responder device 404 (614).

[0167] The responder device 404 can display data from the user device (616) and can receive input to initiate a connection for the user device 402 with another device (618). For example, the responder may determine that the user of the user device 402 has a medical emergency and he/she is unable to request help. The responder device 404 can initiate a connection between the user device 402 and another device 407, such as an emergency responder, a professional security service, and/or an emergency handling system (e.g., E911 system).

[0168] The responder device 404 can transmit instructions to the user device 402 (620), which the user device 402 can receive and use to initiate communication with the other device 407 (624, 626).

[0169] FIG. 7 is a flowchart of an example technique 700 for providing emergency text messaging services on a user device. For example, the technique 700 can facilitate fast yet detailed emergency texts to be generated by the user device 402 and routed to an appropriate emergency responder 409 through use of the responder device 404, which may be a professional security service.

Text911

[0170] The user device 402 can receive selection of an emergency text feature (702) and, in response to receiving the selection, can begin to automatically collect pertinent information for inclusion in the text message. For instance, the user device 402 can determine its current location (704), obtain an image, video, and/or audio of the user, an assailant, and/or the user's current surroundings (706), and access stored information about the user (e.g., name, date of birth, height, weight, medical conditions, emergency contact, telephone number, preferred emergency responders) (708). The user device 402 can receive user input to identify the situation and the assistance that is needed, and/or the user device 402 can receive a selection of one or more predetermined messages (e.g., textual message, video message, audio message) (710). Such input can be textual input (e.g., typing) and/or selection of one or more fields from populated menus. Such fields can include prerecorded messages (textual, verbal, visual) that have been designated by the user and/or by other users. Using the automatically obtained information and the user input information, the user device 402 can generate a text message (712). The user device 402 can also select an appropriate responder to whom the text message should be transmitted (714), which can be similar to the selection described with regard to step 430. Selection of the responder (e.g., steps 430, 714) may additionally and/or alternatively be performed by another computing device that is different from the user device 402, such as by a computer server system. With the text message generated and the recipient selected, the text message can be transmitted to the re-

sponder device 404 (716).

[0171] The responder device 404 can receive the text (718), access emergency routing information (720), and can use the emergency routing information and the information contained in the text message (e.g., location information, type of emergency) to select an appropriate emergency responder to receive the text message (722). The steps 720 and 722 can be performed in a manner similar to steps 552-554. With the emergency responder selected, salient details from the text message regarding the emergency can be routed to the emergency responder 409 (724).

[0172] The emergency responder can receive the information (726) and can respond to the incident (728), such as transmitting a text response to the user device 402, travelling to the user's location, directing others to travel to the user's location, and/or initiating a phone or video conference with the user device 402.

[0173] The responder device 404 can additionally notify the user device 402 that the emergency responder 409 has been contacted (730), such as over a response text message. The user device 402 may receive the contact information for the emergency responder 409 (732) and can initiate contact with the emergency responder 409 (734), such as over a text message, phone call, video conference, and/or security session. The emergency responder 409 can accept the contact from the user device 402 (736). Alternatively and/or additionally, the emergency responder 409 can initiate contact that is accepted by the user device 402.

[0174] FIG. 8 is a flowchart of an example technique 800 for providing real-time crime maps and safety levels to users. The example technique 800 can be performed in part by a central computer system 802 (e.g., central computer system 210, server system 406) and first, second, and third user computing devices 804-808 (e.g., mobile computing device 102, mobile computing device 202, user device 404).

Real time crime reporting, mapping, and notification

[0175] As part of incident reporting and crime map generation, users may upload information regarding incidents that they are aware of. This information may be provided to authorities, or to other users. This information may include their location (which may be determined automatically from their device, including by GPS or WiFi-based location). This information may include the type of incident, their comments, and photos, video or audio or other types of information. This report may be registered or marked automatically on a map that is visible to other users. Reports may be sent automatically to other users, or to other users near to the site of the report. In the depicted example, the first user device 804 reports an incident which is then used to provide an update to the crime map displayed on the second user device 806 and to the safety score for the second user device 806. For instance, the first user device 804 receives an inci-

dent report entered by the user of the first user device 804 (810), which is then transmitted to the central computer system 802 (812).

[0176] The central computer system 802 receives the incident report (814). The central computer server system 802 can provide security alerts to other users based on the incident report, as indicated by steps 815a-c. For example, the computer server system 802 can identify other users to whom the incident may be relevant and/or important (815a), such as users who are currently or are likely in the future (e.g., within a threshold period of time) to be located near where the incident occurred and/or users who are part of a group of predefined users who are identified to receive such reports (e.g., emergency responders, friends of the first user). The central computer system 802 can transmit (e.g., push notification) the alert with the incident report to the identified other users (815b), which in this example includes users who are associated with the second user device 806 and the third user device 808. The second and third user devices 806, 808 can receive and display the alert/incident report, for example, as a push notification (815c).

[0177] The central computer system 802 can also use the incident report to update real-time crime map data that is maintained by the central computer system 802 and used to provide real-time crime maps and safety levels (816). The central computer system 802 uses the updated data to generate and transmit updated map data to the second user device 806, which may receive the updated data based on the second user device 806 being currently located within a threshold distance of where the incident occurred for the first user device 804 (818). The second user device 806 can receive and display the updated map (820) and can additionally provide updated information (e.g., location) regarding the second user device 806 to the central computer system 802 (822).

[0178] The central computer system 802 can receive the current information from the second user device 806 (824) and can determine an updated safety level for the second user device based, at least in part, on the updated crime map data and/or the current information from the second user device 806 (826). The safety level for a user can be determined based on a variety of factors, such as the current location of the user, the time of day, the day of the week, crime information for the surrounding area, recent incidents in the surrounding area, an age of the user, gender, and/or information about available responders (e.g., current availability, proximity to user, time since last active on their device). The central computer system 802 can select significant factors that contributed to the magnitude of the score (e.g., high score indicating that the user is safe, low score indicating that the user is in danger) (828). For instance, a user's score may drop suddenly indicating that he/she is suddenly less safe, and the significant factors that are selected can be those that most contributed to the decline in the score. For instance, if all of a user's responders go offline around the same time, the score for the user may drop and the se-

lected significant factor can be the absence of available responders.

[0179] The safety level may be presented on the user's device in a number of ways. The safety level may be presented as a number. The safety level may be presented as an icon. The safety level may be presented as a color. The safety level may be presented by changing the background image or background color of the screen. The safety level may be presented through text information.

[0180] The score and significant factors can be transmitted to the second user device 806 (830).

[0181] The second user device 806 can display the score and significant factors to the user of the second user device 806 (832).

[0182] The central computer system 802 can proceed to determine whether the score has dropped below one or more threshold levels that can trigger varying levels of safety procedures (834). For example, a first level may result in simply a notice to the user and a second, more serious, level may result in a broadcast to the user's responders in addition to the user. Based on the determination, safety alerts can be transmitted (836) to the second user device 806 and, in some implementations, to a third user device 808 that may have been designated by the second user 806 as a responder. The second user device 806 and the third user device 808 can display the alerts to their respective users (838, 840). In addition, an icon may be presented for a first user on a second user device 806 and the third user device 808 showing a coded or directly represented indication of the safety level of the first user, for example a number, or a color-coded or size-coded representation of the first user's safety level that is displayed on the second user device 806 and the third user device 808.

[0183] FIGS. 9A-F are screenshots of user interfaces that can be presented on computing devices as part of the devices, systems, and techniques described above. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

[0184] FIG. 9A depicts a screen showing remote control features that can a user of the device can select to control the operation of another user's device. The example remote control features include turning a microphone on the other user's device on/off (900), increasing the volume of speakers on the other user's device (902), turning a flashlight on the other user's device on/off (904), switching the camera that is being used on the other user's device (906), taking a picture using a designated camera on the other user's device (908), enabling/disabling an idle timer on the other user's device (910), and playing an audio file on the other user's device (912).

[0185] FIG. 9B depicts a screen showing an example video chat session, which can be one way, two-way, or

multi-way among a plurality of users. In the example screen, the recipient (e.g., the responder) is seeing a real time video (914) from the user's device.

[0186] FIG. 9C depicts a mobile application screen showing example user interface elements. For instance, the depicted elements include, a button to call an emergency responder (916), a "Safe Timer" button that will issue a call to a responder if not cancelled within a specified period of time (918), a "Danger" button that will call a supporter (920), a "Protectors" button that will send a beacon signal to friends and family (922), and a "Call Me" button that will issue a request to receive a phone call within a period of time (e.g., 10 seconds, 30 seconds, 1 minute) (924).

[0187] FIG. 9D depicts a mobile application screen showing user interface elements that include an example element 926 providing localization of a user in real time.

[0188] FIG. 9E depicts a mobile app screen showing user interface elements, such as elements 928 through which the user's information can be entered and elements 930 through which protectors/responders/friends/family/contacts can be identified either from existing data sources (e.g., contacts, FACEBOOK) or entered manually.

[0189] FIG. 9F depicts a mobile app screen showing user interface elements, such as elements through which a user can enter preferences for a period of time to wait before receiving a call back (932) and before calling a police officer (934).

[0190] FIG. 9G depicts a mobile app screen showing user interface elements, such as a real-time video of another user (936).

[0191] FIG. 10 is a screenshot 1000 of a user interface that can be presented on computing devices in Ready Mode. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

[0192] The screenshot 1000 depicts a variety of user interface features, including a flashlight toggle (1002), a button to send emergency messages with user locations to a predefined list of contacts/friends (1004), a button to call emergency response (e.g., 911) from either the user phone or a remote responder (1006), a feature to adjust the video quality/resolution/frame rate (1008), a live video and/or image of an available responder, who may be the nearest available responder or a nearest available responder from a predefined list (1010), information identifying the availability of a responder service at a premium/priced plan (1012), a button to start a call to the responder substantially immediately (1014), a responder name or ID (1016), a button to toggle the user camera (1018), a feature indicating whether the video is being recorded based on whether the light is flashing (red) or continuously (red) (1020), and a continuous video from the user's mobile camera, which may be continu-

ously recorded on the user's device, the responder's device, and/or a remote server system (1022).

[0193] FIGS. 11A-E are screenshots of a user interface that can be presented on computing devices when transitioning from Ready Mode to Caller Mode and Responder Mode. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

[0194] Referring to FIG. 11A, from Ready Mode, a user can select the button 1100 to initiate two-way audio/video communication to enter Caller Mode.

[0195] Referring to FIG. 11B, in Caller Mode (screen seen by the caller) the name/ID of the responder/friend who was called can be displayed (1102), the responder live video can be displayed (1104) (not displayed in audio-only mode, during which a static image may be presented), a terminate connection feature is presented (1106), and self (caller) live video or video looking out at world is presented (1108).

[0196] Referring to FIG. 11C, Responder Mode (screen seen by the responder) is presented, which is entered by the caller pressing the button 1100, sending a push notification, a call request, or connecting a friend/responder. Screen 1110 is initially presented with low quality video of the caller. Using the quality feature 1112, a higher quality video of the caller is presented in screen 1114, as depicted in FIG. 11D. A video of the user's self (responder) is presented in window 1116. In the example depicted in FIGS. 11C-D, the screenshots show the same person as the user of the mobile computing device and the responder for mere illustrative purposes and, in general, the user and the responder will be different people using different devices.

[0197] Referring to FIG. 11E, in Responder Mode with display of a map and menu, a live video of the caller is presented 1118, a menu of remote controls of the caller's device are presented (1120) (e.g., mute, change volume, take a picture which is received by the responder, play audio on the user's device, such as an alarm, verbal commands), and a map of the caller's location, through which the responder can pinch-to-zoom, view the caller's address, and a connection to local 911/emergency center can be provided (1122).

[0198] FIGS. 12A-D are screenshots of a user interface that can be presented on computing devices to initiate and participate in two-way instant messaging. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

[0199] Referring to FIG. 12A, a list of users are presented and a two-way instant messaging session can be initiated by selecting (tapping) a user entry.

[0200] Referring to FIG. 12B, a text message session is depicted with a feature 1200 through which a user can send messages with a variety of information, including userid, user name, geolocation, map, time, date, and/or text message to a peer.

[0201] Referring to FIG. 12C, features are presented through which a request for a video call can be sent, a request for an audio call can be sent, a request for a user's exact location can be sent, or a text message to the entire list of users friends/contacts can be sent (1202), a feature for sorting friends by proximity (1204), a feature through which a friend/user can be selected for participation in instant messaging session, audio call, video call, or other form of communication (1206).

[0202] Referring to FIG. 12D, a map is depicted showing the location of friends, with pictures and name/id, based on their most recent check-in or real-time geolocation from their device (1208). Location services can be requested for a friend and people may turn on/off the ability of other users to view their location and the toggle the level of accuracy of the location being provided to other users.

[0203] FIG. 13 is a screenshot of a user interface that can be presented on computing devices to access several security-related features. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

[0204] Button 1300 accesses a "Personal Bodyguard" screen in which a real police officer, available 24/7, will be presented to address a potential attacker by live, two-way video conferencing that he (the police officer) has already permanently recorded the attacker's face and location, and has stored that information in a secure web location with the assurance that, if any crime is committed, this evidence will be used to convict the attacker.

[0205] Button 1302 accesses a "Text 911" feature through which a user of the device can send a text message to emergency responders. Button 1304 accesses a "Contact Your Hero" screen in which you can contact another user (e.g., friend, loved one, family member) by voice, videocall, and/or text, along with providing your location to that person, allowing that person to converse with people located nearby, and to record the communication feed. Button 1306 accesses a "Personal Security Camera" feature through which video from the device will be permanently recorded on the device as well as at a remote location so that if someone were to approach a user, the user would be able to have a permanent record of what happened, even if their phone was stolen or destroyed.

[0206] FIG. 14 is a screenshot of a user interface that can be presented on computing devices to display and access several security-related features. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile com-

puting device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

[0207] Button 1400 access a "Personal Bodyguard" screen, similar to button 1300. The "Incident Reporting" feature 1402 allows a user to report an unsafe location, crime, accident, or other emergency through the system. Incidents are reported to the appropriate authorities and other users are alerted of the incident to provide notice so as to keep them safe. The "Message All Friends" feature allows for a text message, an audio call request, or a video call request to be sent to all of a user's friends simultaneously, with the first of your friends answering the message/request being available to the user. The "Friends List" feature is a slider that shows all of a user's friend who can be contacted and the user's "hero," who is a designated person who will serve as your first responder. Button 1408 is a "Personal Security Camera" feature similar to the button 1306. Friends Map 1410 is a map that displays real-time locations and status information relating to a user's friends. The view of the map can be changed in a variety of different ways, such as through scrolling, panning, and pinch-to-zoom interactions.

[0208] FIG. 15 is a screenshot of a user interface that can be presented on computing devices during a 2-way video chat. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

[0209] The "Record to Cloud" feature allows for videos taken by a user's computing device, such as during a call, to be recorded directly to a remote storage location (e.g., the cloud) in a secure manner (e.g., calls and data are secure and encrypted). The "Opponent Video/Audio" feature 1502 is a real-time video display over which a user can see and hear his/her friend/hero/trained responder by two-way video conferencing using any of a variety of data connections, such as WiFi and/or cellular networks.

[0210] FIG. 16 is a screenshot of a user interface that can be presented on computing devices to display and access several security-related features. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

[0211] The map 1600 can display real-time locations of a user's friends. The "More Ways to Help" feature 1602 allows for a user to perform operations for other users (e.g., friends, family members, contacts). To access this feature, the other user that a user would like to help may need to have provided permission for the user to help

the other user. For example, a user can use this feature to have a responder call the other user, send a safety message to the other user's friends, send a call request to the other user's friends, and/or other features. The "Auto Answer" feature 1604 allows a user, when given appropriate permissions, to initiate a video or audio call on another user's computing device without the other user needing to first answer the call. For example, a user can start audio and/or video communication with another user's device even if they are not able to press a key to accept the call. The "Responder Call" feature 1606 places a call directly from another user's device (e.g., friends' phone) to a responder so that the responder can pick up and engage the other user. The "Contact Friend" feature allows a user to audio call, video call, send a text message, and/or send a user's location to another user.

[0212] FIG. 17 is a screenshot of a user interface that can be presented on computing devices to report an incident. For example, the screenshots can be presented on any of a variety of appropriate computing device, such as the mobile computing device 102, the mobile computing device 202, the user device 402, the responder device 404, the other computing devices 108a-d, and/or the other computing devices 204.

[0213] The "Report an Incident" feature 1702 can map the location of an incident based on the location of the computing device and/or manual location entry. The "Submit to Cloud" feature 1700 can upload information about an incident, such as the type of incident, photos, video, audio, and/or user comments. Alerts can be sent to appropriate authorities and/or other users in response to an incident being reported.

[0214] FIGS. 18A-B are a screenshot of a user interface through which a user can enter their profile information and register to use the security features discussed above.

[0215] FIG. 19 is a screenshot of a user interface that depicts a safety level indicator 1900 for the user of the computing device displaying the user interface as well as safety level indicators 1902a-d for the user's acquaintances, who identified at their recent/current locations on the map 1904. In the depicted example, the safety levels are identified by colors, such as green (safe), yellow (moderately safe), and red (unsafe). Other scales and intermediate levels are also possible, as well as other ways of indicating differing safety levels, such as numerical scales (e.g., scale of 1-10 in which 1 is unsafe and 10 is safe), textual descriptions (e.g., words "safe" and "unsafe"), and other user interface elements to convey to a user of the computing device safety levels for the user and his/her acquaintances. As discussed above, the safety level may be determined on the user device and/or by other computing devices (e.g., central server system) based on any of a variety of appropriate factors, such as whether the app active on their computing device (e.g., when was the last time their location updated), the current time (e.g., daytime, nighttime), whether the user is at or near one or more known safe locations (e.g.,

home, work, other defined positions in a user's profile), whether and how many of the user's acquaintances are available/online in the app, whether the user is currently located in a dangerous neighborhood (e.g., based on imported this crime/map data), and/or other relevant factors.

[0216] In one example use case, a user might want to see whether his/her children are safe and can do so by looking at their safety levels on the application. If anyone is red or yellow, the user can take action to find out what is going on and, possibly, assist the user through any of a variety of the features described above, such as auto-answer and remote control. In another example use case, the a user can have an alarm set on the app so that if a friend drops below a green safety level that a notification is automatically generated. The notification can prompt the user to examine the friend's status and to possibly take action to assist the friend.

[0217] A variety of additional features can be used in combination and/or alternatively to the features discussed above. For example, rewards and/or incentives can be offered and awarded for finding and/or capturing assailants identified through the technology discussed above. For example, a rewards/incentives system may be used to provide information or incentives to support others in supporting the user (including finding the user), or in capturing an assailant or other criminal involved in an incident. For example, the user may provide information and/or a reward for the capture of an assailant. For example, the user's support network/contacts may provide information and/or a reward for finding or assisting the user if they are lost or in an emergency situation. Bounties for leading to the identification and/or capture of an assailant may be made public or private (e.g., shared with a user's social network, close friends, family).

[0218] FIG. 20 is a screenshot of an example home screen for a mobile security application that includes features to send a text to 911 (2000), securely record video and/or audio to a cloud storage device (2002), view the location and status of acquaintances and/or responders (2004), select one or more acquaintances and/or responders (e.g., slider feature) (2006), contact a particular responder (2008), and view available responders (2010). These features can be static and/or dynamic. For example, the feature 2004 may show an updated map with nearby and current acquaintance/responder locations.

[0219] FIG. 21 is a screenshot of an example user interface through which a user can enter and transmit a text message to emergency responders, such as 911 emergency services. The example user interface includes a text field into which a user can type a message (2100), a button to send a text message to emergency responders (2102), a dropdown menu through which a user can select one or more predefined incident types (e.g., crime, medical emergency, accident) (2104), an interface through which a picture, video, or other media (e.g., audio file) can be captured and/or selected for transmissions (2106), a selectable feature through which

a user can indicate whether police or other emergency services should be dispatched to the user's location (2108), and a selectable feature through which a user can indicate whether police or other emergency services can call the user for further details (2110). Other features can also be included in the user interface that are not depicted in this screenshot, such as depicting a map of the user's current location, which can be modified and/or annotated (e.g., add location identifiers and descriptions to map) by the user and captured for transmission to the emergency service (e.g., screenshot of the map as modified/annotated by the user); fields through which a user can select and/or enter his/her current address; and/or a button through which a user can record a voice message that is either sent as audio or as text (using speech to text) to other users.

[0220] An affiliate program may be used to provide rewards (e.g., money, credits, free services) to users who refer the service to other users who sign up. For example, users may broadcast the service to their acquaintances on one or more social networks. Compensation may be provided beyond first level recipients of the referral. For instance, second tier acquaintances (friends of friends) who sign up may provide compensation to the original user who promoted the service, but at a lower level of compensation than for first tier acquaintances. Such tiered sharing/promoting of the service can be used to provide a user with a personal impact map that depicts the locations of people who signed up based on their referral, either directly or indirectly. Users signing up may be color coded based on the level at which they were referred by the original user (e.g., first tier referrals can be red, second tier referrals can be orange, third tier referrals can be green).

[0221] In another example, black box style tracking of a mobile device can be used to provide information about the user's situation at a later time that has been transmitted to a remote location, such as the user's locations, battery levels, photos, audio, video recorded from the device, calls, texts, other activities that may be helpful in determining if the user is safe or in danger, and their location.

[0222] In another example, particular billing and business practices can be used to charge users for this service and technology on a subscription basis. For example, users may be charged for the purchase or use of this technology, may be charged based upon connection time, recording time or volume, or number of connections, or a combination of these.

Virality, Affiliates

[0223] Users of this system may be encouraged to have their family or friends also sign up to use this service, and to download apps/software to do so. They may be provided with incentives to engage others in this service. It may be that the family or friends need software or hardware provided by this invention to most effectively sup-

port the user (for example receiving real time push notifications, map locations for the user, one-way or two-way video, etc.). This may also allow the family or friends to thereby become users themselves. The family or friends of a user may be able to have access to the users information, or they may only have access to select information about the user, as selected by the user in their preferences, or they may only have access to the information about a user at times or circumstances selected by the user (e.g. if the user has indicated an emergency, then their contacts get access to their location or other information), or they may only have access to the information about a user at times or circumstances selected by an emergency responder (e.g. if the emergency responder has indicated an emergency, then their contacts get access to their location or other information), or they may only have access to the information about a user at times or circumstances selected by another contact or member of this service (e.g. if a selected contact or service provider has indicated an emergency, then their contacts get access to their location or other information).

Pricing

[0224] All of the services in this invention may be priced separately, or provided for free, or bundled into different plans, or service levels, or using tiered pricing, or using country-specific or location-specific pricing. In one embodiment, features requiring recording or storage of certain information may be priced at a premium. In one embodiment, features requiring a human responder may be priced at a premium. In one embodiment, users may be charged a daily, weekly, monthly or yearly subscription fee for the use of the service. In one embodiment, users may be charged a per-minute, per-hour, per-day, per-week, per-month, or per-year usage fee for using any of the technologies features. For example, a user may be charged per-minute for recording in ready mode, for having access to a responder in ready mode, or for being in communication with a responder in ready mode.

Licensure

[0225] In one embodiment, this technology may be provided as part of a licensed service, including licensing the provider as a private patrol operator, burglar alarm or other alarm company, personal emergency response service company, private security or bodyguard company, or other types of licensing in certain jurisdictions. In one embodiment, this technology may be provided as part of a licensed service, including licensing the provider company as a private patrol operator, burglar alarm or other alarm company, personal emergency response service company, private security or bodyguard company, or other types of licensing in certain jurisdictions.

Geofencing and/or location of user

[0226] In one embodiment, certain aspects of the service may be provided only when a user is in a given jurisdiction, or within another geographically-defined region (for example using geofencing) where the provider is appropriately licensed to provide this service. Examples of appropriate licensing include holding a state burglar alarm license, a private security license, or a personal emergency response system (PERS) license. In addition, in one embodiment the service selects a responder who is appropriately licensed for the jurisdiction that a user is physically located in. For example, if a user is located in the state of California, a responder is selected who is appropriately licensed to operate in the state of California. This selection of the responder may involve looking up responder licensing information for each responder in a database stored on a server, or using data on the mobile device of the responder. Responder groups may be defined that include responders licensed for certain jurisdictions, and when a user is in that certain jurisdiction, they may be connected with responders within a responder group appropriate for, or licensed in, that jurisdiction.

[0227] In one embodiment, the provision of service may be restricted to certain geographic regions where the user is located. In one embodiment, certain aspects of the service may be provided only when a user is in a given state, country, municipality, within a set distance of a defined position, or within another geographically-defined region (for example using geofencing).

[0228] In one embodiment, the user's location, user's language or user's language-preference may be used to select a responder based in part based upon the responder's spoken language(s) or the responder(s) location.

Examples of Hardware and Software

[0229] This disclosed technology provides for a number of different hardware devices, software applications, databases, connections, and other technologies that may be used alone or in combination. These include: mobile computing devices (e.g., mobile phones, tablets, cameras including video cameras, wearable computing devices, PDA's and other current or future devices), connection hardware (e.g., devices that may communicate via any type of existing or future wired or wireless communication method, including WiFi, Cellular (3G, 4G, LTE, 5G, etc.), internet, web, Bluetooth, etc.), web devices and/or computers (e.g., computers, servers, databases, and other hardware and software, such as computers and servers that run software that communicates and/or stores the information described), networks (e.g., wired and/or wireless networks including peer-to-peer, server-client, and other network architectures), cameras and microphones (e.g., any type of camera, microphone, speaker, lights, monitor for collecting and communicating information, such as public and/or private security cam-

eras, cameras in the immediate vicinity of the user (based on the localization of the user and the cameras) may be used to gather further information about the user, or to display it to the responder or users contacts/supporters), drones (e.g., controlled or automatic drones that may collect or transmit information, such as automatic drones that are dispatched to the location of the user to provide real time video of the situation), and/or software.

[0230] Such software can include apps running on the users device, such as apps with videochat, recording, and other functionality as described, apps running on the responders device, such as apps with videochat, recording, and other functionality as described, and/or website for users. A website may be provided to allow users to do things including: sign-up, provide their information; and register their mobile device(s), select and contact members of their contact list, friends (including Facebook friends or contacts from other devices or social networks), family and supporters; track all new users or prospects contacted by a user, and it may track the ones contacted by them, so that the full diaspora of users contacted directly or indirectly by a single user may be determined, and statistics, locations, numbers may be presented to the user or others. This may also be used to incentivize a user to contact others, e.g. through affiliate marketing or direct sales approaches. Other measures of the spread of the technology and its virality may also be used, such as viral coefficients and social graphs. In another example, the software may be programmed to view or share information that they have recorded during prior incidents, such as audio/video, maps of their location, to view or share information recorded or shared by other users (e.g. re-sharing information), to pay or receive payment for the use of this service, or pay for calls/time or other content, to be a website for responders (e.g. a website may be provided to allow responders/supporters to do things including: sign-up, provide their information, register their mobile device(s), select and contact other users who have selected them to be supporters or responders, such as their friends, family, or members of the public, view or share information that they or users have recorded during current or prior incidents, such as audio/video, maps of their location, and/or pay or receive payment for the use of this service, or pay for calls/time or other content). The software can additionally include social network/social network apps for users/responders. These will allow users, their networks, and responders to communicate and to share information from this invention.

[0231] The disclosed technology can also be used on non-mobile computing devices, such as desktop computers, either through dedicated software, or through a web browser, or through a portal or social network app. For example, a desktop computer can be used to do things like send out a request for connection through a social network, and have the recipient click a link that starts an app (including one that is hosted remotely so that they don't have to download it) and allows them per-

form the functionality discussed throughout this document. Such interaction on a desktop computer can be performed by a webapp, which can be run within a web-browser, within dedicated software, and/or through social media applications (e.g., FACEBOOK app).

WebRTC, HTML5, browser and social functionality

[0232] Additional technical features that can be used to implement this technology include WebRTC, which may be adapted with specialized code for cross-platform used, and Hybrid HTML5, which can allow for access to both native and HTML5 functionality on mobile devices. Plugins of such technologies or different technologies may also be used. WebRTC may be used for secure transmission of data, audio, video, messages, including two-way videochat, audiochat, and messaging. This information may all be recorded either locally on a user's device or responder's device. This information may all be recorded simultaneously to a remote server, including by initiating an additional webRTC connection to said remote server that streams all data to the remote server simultaneously with the two-way communication between a user and a responder. WebRTC can be used with the disclosed technology to securely transfer audio, video, data, messages, locations, images. This can be done in web browsers, using HTML5, in native IOS, ANDROID, Windows Phone, or other appropriate code. Plugins can also be used, such as those for Phoneygap, Titanium, and/or Intel XDK.

[0233] The disclosed technology may additionally include a personal alarm light. This alarm light may include a flashing light. In one embodiment, this may be the 'flashlight' of a mobile phone, programmed to have a repeating flash pattern. This repeating flash pattern maybe 800msec on, 200msec off duty cycle. This repeating flash pattern maybe 500,600,700,800,900,950,990 msec on, and the balance of one second off. This flash pattern may serve as an indication that a user is using the technology. For example, this flash pattern may serve as an alarm warning light.

Device Carriers and Holders

[0234] The disclosed technology may additionally be combined with physical holsters/carriers that can be used to obtain consistent recording of a user's surrounding environment for a particular use. For example, a lanyard can be used to allow for hands free recording and operation of a mobile device. In another example, a dash cam mount can be used to allow for hands free recording while operating a vehicle. These holsters/mounts can include battery extensions (back-up power sources) and the placement of a device in these units may be detected by the device, which may in turn automatically enter a particular mode of operation.

Notifications Based on User Location

[0235] The disclosed technology may additionally include providing notifications when a user arrives at a particular geographic location or area. For example, when a user arrives home at the end of the night, a notice of the user's safe arrival may be provided to one or more other users/responders. Selection and designation of such a target location for notification can be performed by a user him/herself or by another users (e.g., responder). Additional alarms may be set and triggered if the user does not arrive at his/her destination by a particular time or within a particular window of time. In response to a user not arriving at a particular location within a particular time, other users may be notified and/or may automatically be entered into a communication session (e.g., text message session, video chat) with the user.

Training, Exercises

[0236] The disclosed technology may additionally include one or more training exercises to educate users on how to properly use the technology in the event of an emergency. Such exercised may take the form of text, audio, or video. Such exercised may take the form of games, simulations, or exercises. These simulations may train the user in scenarios designed to be similar to real-world emergency scenarios, so that in the event of a real emergency a user will already know how to react. In one example game, similar to the common game 'assassin' or 'killer', each user in a group may receive the name of another user in the group, with no users knowing who has their name. The objective of the game can be to tag the person whose name a user has by capturing a sufficiently clear and steady image or video of that user. Once that user has been tagged, then the user gets the name of the person they just tagged to be their next objective. The game can continue until there is one remaining player. The game can teach users how to properly operate the device under physically stressful and chaotic situations, which may mirror a real life scenario.

Games

[0237] In one example of a game, which may be used in training users to use this technology, augmented reality may be used to simulate situations of emergencies, crimes, or assaults. The user may use their device within the game in a similar way to which they would use their device in a real emergency situation. The user may receive a score, or feedback, based upon how well they used the device in the simulated situation. In one example of an augmented reality game the video camera of a mobile device may be used to simulate a gun (similar to the augmented reality game phoneygun or a first person shooter type game), or to simulate a camera on which a user must 'catch' (by photographing or capturing on video) another user or a specified object or location.

Social Networks

[0238] This technology can be integrated with one or more social networks (e.g., FACEBOOK, TWITTER), such as for communication, status information, message broadcasting, and other features. Privacy of the users can be maintained, with access to a user's personal data and device access being restricted to only those users or user roles (e.g., fireman, police officer) that the user has explicitly designated. Additionally, the technology may not allow for a remote user to gain access to any private data that may be stored on a user device. The communication, settings, and automatic determinations that are made by this technology can be transparent and clearly identified to users.

[0239] A link or invitation may be sent to a first user to directly initiate a communication session with a responder. This link may be sent by email, SMS/text message, social network, or other electronic means. When the responder receives the link, including whether or not they have software installed on their local machine, they may click on the link or otherwise initiate communication using software that is stored on their local device, or software that is stored remotely from them and served to them via computer network. This may include either the user or the recipient using browser or social network plugins.

Lie Detection, Other Forms of Evidence

[0240] This technology may additionally be used in conjunction with lie detection technology, such as lie detection based on physical changes and stresses, such as blood pressure changes, breathing rate changes, heart rate changes, vocal pattern changes, and/or changes in eye movements, or brain wave (EEG, HGI) or brain scanning technologies. For example, if someone is identified as a suspect in a crime or other event using the technology, this may be verified at a later time through lie detection technology. This technology may additionally be used in conjunction with other forms of evidence, for example forensic evidence, DNA evidence, digital surveillance evidence, location evidence or others. In one example, if someone is identified as a suspect in a crime or other event using the technology, this may be verified at a later time through corroboration with other forms of evidence.

Incentive Program

[0241] An incentive program can be provided to encourage participation and assistance of other users. For example, users could receive rewards (e.g., awards, badges, points, financial rewards, credits towards payment for software or use of services, credits towards payment for time using this technology) for contacting another user to inform them of the application, for encouraging them to download or sign up for the application, or for assisting another user in need through using the ap-

plication. Such rewards could be redeemed for something (e.g., travel voucher, gift card) or publicized (e.g., press release with user's consent, national/regional award for good Samaritan). For example, a user could have displayed on a webpage how many other users they have invited to use this system, or how many other users they have as 'Friends' within this system, or how many other users have selected them as a responder or to be on a responder list.

Additional Data Sources for Geotargeted Alerts

[0242] Additional and/or alternative data sources can be used to provide geotargeted alerts to users who are located within one or more relevant geographic locations. For example, data sources providing information about emergencies (e.g., national emergency monitoring system) and/or weather-related events (e.g., weather/meteorological systems) can be accessed or can push information to this system and, when an event with at least a threshold predicted or occurring level of severity is identified, users that are located inside or within a selected distance from the affected area can receive an alert (e.g., message, recorded message, push notification) to inform them of the event, and people whom they have designated (for example their friends) can also receive a notification.

[0243] This technology can also be used with prosthetic devices, such as prosthetic devices that are controlled through brain-computer interfaces (BCIs). Aspects of the device may be controlled by BCI rather than a conventional user interface such as a touch screen. For example, data from such prosthetic devices may be provided to and used by the technology described above.

Speech to Text/Text to Speech, and Translations

[0244] Where appropriate, speech to text and text to speech technology can be used to convert speech to text for transmission/presentation to other users/devices, and to convert text to speech for presentation on user devices. Speech to text and text to speech operations can be performed locally on a user's computing device and/or remotely on one or more remote computer systems (e.g., central computer system). Additionally, translations from one language to another can be performed on speech and/or text, so as to facilitate communication between users speaking different languages. Likewise, such translations can be performed locally and/or remotely from a user computing device.

Facilitating Cross-Jurisdictional Assistance

[0245] As discussed above, the ability of a responder to assist within a particular jurisdiction based on licensure may be checked before connecting a user with that responder. Cross-jurisdictional assistance (e.g., responder outside of user's jurisdiction providing assistance

through application) may be facilitated by providing a variety of features, such as through recording security sessions, providing information to emergency authorities about ongoing cross-jurisdictional assistance, providing information to a court (e.g., to get approval), providing the responder with access to an appropriate PSAP for the user, using Ready Mode, allowing the responder to be automatically selected from a list, allowing the responder to see user's location, including as it changes and during video connection, the ability to 'cancel' repeated signals from a caller, rather than contact 911 multiple times, and/or the ability to follow up with the user later/the next day.

Call Center, QA/QC

[0246] In an example use case, the disclosed technology can be used in with call center and QA/QC functionality. For example, the disclosed technology provides for a network of responders working in a call-center environment, or working remotely at dispersed locations. The technology may be used in combination with all aspects of call center technology and best practices. Some aspects are described in: Call Center Management on Fast Forward: Succeeding in the New Era of Customer Relationships (3rd Edition) by Brad Cleveland, Layne Holley and Michael Blair (May 8, 2012), included by reference.

[0247] In particular, the technology provides for: recording/archiving of the incoming and outgoing communication by each responder and for each user, rating/grading of each communication and each responder by users or by other raters, measurement of all parameters of each call and each responder including those typically used in call centers, including average utilization, latency to answer, length of call, quality of interaction, time to dispatch services, time to determine and document nature of call, and others. For remote responders, including responders to the scene, measurement of time from when call was received until responders arrived on scene, performed their duties can be made. This measurement may include determination of time of arrival on scene using localization technology as provided.

One-to-Many, Many-to-One, Many-to-Many

[0248] In another example, the disclosed technology can be used in a variety of different communication contexts, such as one to many, many to one, and many to many communications. For example, a single user may use this technology to communicate any of the information described to a plurality of recipients, either in real time or later.

[0249] A plurality of users may use this invention to communicate any of the information described to a plurality of recipients, either in real time or later. For example, many users at an emergency scene may all be videotaping the scene from different angles. A single responder, or a team of responders, may select all of these users

and see all of their information in coordination, for example on the same screen. This technology provides for selecting which users to coordinate in this way.

[0250] A single responder may use this technology to communicate any of the information described to a plurality of users, either in real time or later. For example, if many users are at the same crime scene, a single responder may use their locations to determine that they are all at the same scene, and to handle the situation in a unified way, communicating with all of the other users at the scene, or selecting all users within a fixed distance from a chosen point, and all of the other responders involved in the incident. The responders, or users, may select which other users or responders to including in one-to-many or many-to-many communication.

[0251] It is possible to use this technology for many to many communication, so that for a given group of users and responders, all information communicated by one member of the group is communicated to the others, in real time or later, so that the group may coordinate their efforts. This may take place by group audioconference or videoconference or text message or recorded audio message. This may take place by group members sending information to other members of the group for later retrieval, for example sending group messages, notifications, emails, etc.

With Other Services Including Security, Government, Emergency Responders, Military

[0252] In another example use, this technology can be used for coordination with other services including government services. For example, this technology provided here may be used in combination with other service providers. These may include:

Security companies. This technology may be used in combination with existing security services. For example, fixed security cameras can be augmented with this technology so that while someone is being monitored on a security camera, a security guard or police officer can interact with that person by one-way or two-way audio or video.

Government Emergency Call Centers. This technology may be used in combination with emergency dispatch centers (e.g. US 911 centers). Calls, information, video, audio, text messages, user location and information may be manually or automatically routed directly to a government emergency call center for further processing or dispatch of emergency personnel or other reasons.

Military Communication. This technology may be used in combination with military communication networks and in military contexts. Calls, information, video, audio, text messages, user location and information may be manually or automatically routed di-

rectly to a military emergency network or call center for further processing or dispatch of personnel or other reasons.

Direct communication with responders. Information may be provided directly to emergency responders. For example, if an emergency signal is sent out by a user, it may go directly to the mobile device of nearby police, providing them with any important captured information, including but not limited to the location of the user having the emergency, the identifying information of the user, any video, photos, or audio about the incident, or other useful information. This may help the responders to aid a user or victim, or to apprehend a suspect. The hardware and software may automatically detect the available responders closest to or in the best position or skills to aid with the incident.

[0253] In another example, this technology may be used in war, combat, disaster and anti-terrorism situations. For example, the technology provided herein may be used in military, police, war, combat, disaster and anti-terrorism situations to provide important information in real time and aid in these situations. Information from multiple users may be coordinated by central locations, for example displaying on a centralized map where all responses or users are coming in from, and allowing communication amongst them. This technology may have application in preventing violence within the military, including preventing violence against women perpetrated by other members of the military. This technology may also be used in real or simulated military or combat environments, including in military training, or war games, including civilian combat games like paintball, laser tag or others to coordinate teams, determine locations of users, and allow single or group communication by audio, video, text message or use of the other technology features.

Demonstration of Innocence or Guilt

[0254] This technology may be used to demonstrate a user's innocence (or guilt) in a crime or other incident. For example, if a user is using this technology, and this verifies the user's location at the time of a crime as being distant from the crime scene, this may be used to establish the innocence of the user. This may be enhanced through verification technologies that ensure that the user is physically present at the same location as the mobile device that is transmitting the location, including biometrics such as a fingerprint scanner, an iris scanner, face recognition or capturing an image or video of the user. In addition, this may be enhanced through verification technologies that are physically attached to the user, such as an ankle bracelet that communicates with the device through a wireless connection and verifies that the user is at the same location as the device, and thereby

verifies that the user was or was not at a crime scene.

Lite Messaging

5 [0255] This technology may allow a user to send a "lite" message to initiate communication with other users in a manner that does not require the other users to have a particular application installed on their computing devices - allowing users to rely on and use the participation of other users who have not installed or registered to use 10 a particular application (e.g., mobile security app). For example, a user can send out a lite message, for example, over email, SMS, social network messaging (e.g., FACEBOOK messaging, TWITTER), with the message 15 including a selectable feature (e.g., link) that the recipient can select to immediately begin a connection with the sending user using existing technology on the recipient user's device (e.g., connection without the recipient user having to download/install a particular application). Selection of 20 such a link can cause the recipient's device to identify one or more compatible technologies to use to communicate with the sending device. Such lite messaging can allow for users to send messages that create such links between the two users and to be able to use the functionality very easily and without much interaction by the 25 recipient user (e.g., able to connect with sender with no more than 1, 2, 3, 4 clicks and/or 0,1,2,3,4 entered pieces of identification or information). In one example, a user (calling user) can send a message including a URL link 30 through a messaging platform (email, SMS, Facebook, others) to a responder. This URL link can contain information specifying the sender, or the sender and responder, or the sender, responder. The URL link can also optionally include additional information, including information 35 about the kind of communication being requested, the nature of the situation or topic of communication, the means of communicating, the locations of one or both users, encryption information (for example including a public key), or other information. When the responder 40 receives this message, the responder can click on the URL link. This can bring up in the responders browser a way to communicate with the user who sent the message. For example, the responder's click's the link this can bring up on the responder's browser or on other software on 45 their desktop, mobile device, tablet or wearable device a web page, an app, a widget, or another way for them to communicate with the calling user who sent the message. This web page, an app, a widget, or another way for them to communicate with the calling user may not 50 require download if sufficient resources are already available on the responder's device. If sufficient resources are not available, then those resources may be provided to the responder, for example by the responder clicking on the link, for example by a website being sent to and 55 displayed for the responder. This may not require the responder to take additional steps to install software on his device. When this web page, app, widget or way for the responder to communicate with the calling user is

displayed, it can already be connected with the user who sent the message, or it can pre in a state ready to quickly form that communication connection, for example it can be pre-populated with the calling user's id or network address. The web page, app, widget or way for the responder to communicate with the calling user can display a message asking the responder if the responder would like to communicate with the calling user, or this communication can be begun automatically. If the responder selects that they do want to communicate with the calling user, then communication can be begun.

[0256] The disclosed technology may be implemented as part of a mobile personal emergency response system (PERS).

[0257] Computing devices and computer systems described in this document that may be used to implement the systems, techniques, machines, and/or apparatuses can operate as clients and/or servers, and can include one or more of a variety of appropriate computing devices, such as laptops, desktops, workstations, servers, blade servers, mainframes, mobile computing devices (e.g., PDAs, cellular telephones, smartphones, and/or other similar computing devices), computer storage devices (e.g., Universal Serial Bus (USB) flash drives, RFID storage devices, solid state hard drives, hard-disc storage devices), and/or other similar computing devices. For example, USB flash drives may store operating systems and other applications, and can include input/output components, such as wireless transmitters and/or USB connector that may be inserted into a USB port of another computing device.

[0258] Such computing devices may include one or more of the following components: processors, memory (e.g., random access memory (RAM) and/or other forms of volatile memory), storage devices (e.g., solid-state hard drive, hard disc drive, and/or other forms of non-volatile memory), high-speed interfaces connecting various components to each other (e.g., connecting one or more processors to memory and/or to high-speed expansion ports), and/or low speed interfaces connecting various components to each other (e.g., connecting one or more processors to a low speed bus and/or storage devices). Such components can be interconnected using various busses, and may be mounted across one or more motherboards that are communicatively connected to each other, or in other appropriate manners. In some implementations, computing devices can include pluralities of the components listed above, including a plurality of processors, a plurality of memories, a plurality of types of memories, a plurality of storage devices, and/or a plurality of buses. A plurality of computing devices can be connected to each other and can coordinate at least a portion of their computing resources to perform one or more operations, such as providing a multi-processor computer system, a computer server system, and/or a cloud-based computer system.

[0259] Processors can process instructions for execution within computing devices, including instructions

stored in memory and/or on storage devices. Such processing of instructions can cause various operations to be performed, including causing visual, audible, and/or haptic information to be output by one or more input/output devices, such as a display that is configured to output graphical information, such as a graphical user interface (GUI). Processors can be implemented as a chipset of chips that include separate and/or multiple analog and digital processors. Processors may be implemented using any of a number of architectures, such as a CISC (Complex Instruction Set Computers) processor architecture, a RISC (Reduced Instruction Set Computer) processor architecture, and/or a MISC (Minimal Instruction Set Computer) processor architecture. Processors may provide, for example, coordination of other components computing devices, such as control of user interfaces, applications that are run by the devices, and wireless communication by the devices.

[0260] Memory can store information within computing devices, including instructions to be executed by one or more processors. Memory can include a volatile memory unit or units, such as synchronous RAM (e.g., double data rate synchronous dynamic random access memory (DDR SDRAM), DDR2 SDRAM, DDR3 SDRAM, DDR4 SDRAM), asynchronous RAM (e.g., fast page mode dynamic RAM (FPM DRAM), extended data out DRAM (EDO DRAM)), graphics RAM (e.g., graphics DDR4 (GDDR4), GDDR5). In some implementations, memory can include a non-volatile memory unit or units (e.g., flash memory). Memory can also be another form of computer-readable medium, such as magnetic and/or optical disks.

[0261] Storage devices can be capable of providing mass storage for computing devices and can include a computer-readable medium, such as a floppy disk device, a hard disk device, an optical disk device, a Microdrive, or a tape device, a flash memory or other similar solid state memory device, or an array of devices, including devices in a storage area network or other configurations. Computer program products can be tangibly embodied in an information carrier, such as memory, storage devices, cache memory within a processor, and/or other appropriate computer-readable medium. Computer program products may also contain instructions that, when executed by one or more computing devices, perform one or more methods or techniques, such as those described above.

[0262] High speed controllers can manage bandwidth-intensive operations for computing devices, while the low speed controllers can manage lower bandwidth-intensive operations. Such allocation of functions is exemplary only. In some implementations, a high-speed controller is coupled to memory, display 616 (e.g., through a graphics processor or accelerator), and to high-speed expansion ports, which may accept various expansion cards; and a low-speed controller is coupled to one or more storage devices and low-speed expansion ports, which may include various communication ports (e.g., USB, Bluetooth, Ethernet, wireless Ethernet) that may be cou-

pled to one or more input/output devices, such as keyboards, pointing devices (e.g., mouse, touchpad, track ball), printers, scanners, copiers, digital cameras, microphones, displays, haptic devices, and/or networking devices such as switches and/or routers (e.g., through a network adapter).

[0263] Displays may include any of a variety of appropriate display devices, such as TFT (Thin-Film-Transistor Liquid Crystal Display) displays, OLED (Organic Light Emitting Diode) displays, touchscreen devices, presence sensing display devices, and/or other appropriate display technology. Displays can be coupled to appropriate circuitry for driving the displays to output graphical and other information to a user.

[0264] Expansion memory may also be provided and connected to computing devices through one or more expansion interfaces, which may include, for example, a SIMM (Single In Line Memory Module) card interfaces. Such expansion memory may provide extra storage space for computing devices and/or may store applications or other information that is accessible by computing devices. For example, expansion memory may include instructions to carry out and/or supplement the techniques described above, and/or may include secure information (e.g., expansion memory may include a security module and may be programmed with instructions that permit secure use on a computing device).

[0265] Computing devices may communicate wirelessly through one or more communication interfaces, which may include digital signal processing circuitry when appropriate. Communication interfaces may provide for communications under various modes or protocols, such as GSM voice calls, messaging protocols (e.g., SMS, EMS, or MMS messaging), CDMA, TDMA, PDC, WCDMA, CDMA2000, GPRS, 4G protocols (e.g., 4G LTE), and/or other appropriate protocols. Such communication may occur, for example, through one or more radio-frequency transceivers. In addition, short-range communication may occur, such as using a Bluetooth, Wi-Fi, or other such transceivers. In addition, a GPS (Global Positioning System) receiver module may provide additional navigation- and location-related wireless data to computing devices, which may be used as appropriate by applications running on computing devices.

[0266] Computing devices may also communicate audibly using one or more audio codecs, which may receive spoken information from a user and convert it to usable digital information. Such audio codecs may additionally generate audible sound for a user, such as through one or more speakers that are part of or connected to a computing device. Such sound may include sound from voice telephone calls, may include recorded sound (e.g., voice messages, music files, etc.), and may also include sound generated by applications operating on computing devices.

[0267] Various implementations of the systems, devices, and techniques described here can be realized in digital electronic circuitry, integrated circuitry, specially

designed ASICs (application specific integrated circuits), computer hardware, firmware, software, and/or combinations thereof. These various implementations can include implementation in one or more computer programs that are executable and/or interpretable on a programmable system including at least one programmable processor, which may be special or general purpose, coupled to receive data and instructions from, and to transmit data and instructions to, a storage system, at least one input device, and at least one output device.

[0268] These computer programs (also known as programs, software, software applications, or code) can include machine instructions for a programmable processor, and can be implemented in a high-level procedural and/or object-oriented programming language, and/or in assembly/machine language. As used herein, the terms "machine-readable medium" "computer-readable medium" refers to any computer program product, apparatus and/or device (e.g., magnetic discs, optical disks, memory, Programmable Logic Devices (PLDs)) used to provide machine instructions and/or data to a programmable processor.

[0269] To provide for interaction with a user, the systems and techniques described here can be implemented on a computer having a display device (e.g., LCD display screen, LED display screen) for displaying information to users, a keyboard, and a pointing device (e.g., a mouse, a trackball, touchscreen) by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any form of sensory feedback (e.g., visual feedback, auditory feedback, and/or tactile feedback); and input from the user can be received in any form, including acoustic, speech, and/or tactile input.

[0270] The systems and techniques described here can be implemented in a computing system that includes a back end component (e.g., as a data server), or that includes a middleware component (e.g., an application server), or that includes a front end component (e.g., a client computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the systems and techniques described here), or any combination of such back end, middleware, or front end components. The components of the system can be interconnected by any form or medium of digital data communication (e.g., a communication network). Examples of communication networks include a local area network ("LAN"), a wide area network ("WAN"), peer-to-peer networks (having ad-hoc or static members), grid computing infrastructures, and the Internet.

[0271] The computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

[0272] The above description provides examples of some implementations. Other implementations that are not explicitly described above are also possible, such as implementations based on modifications and/or variations of the features described above. For example, the techniques described above may be implemented in different orders, with the inclusion of one or more additional steps, and/or with the exclusion of one or more of the identified steps. Additionally, the steps and techniques described above as being performed by some computing devices and/or systems may alternatively, or additionally, be performed by other computing devices and/or systems that are described above or other computing devices and/or systems that are not explicitly described. Similarly, the systems, devices, and apparatuses may include one or more additional features, may exclude one or more of the identified features, and/or include the identified features combined in a different way than presented above.

[0273] Features that are described as singular may be implemented as a plurality of such features. Likewise, features that are described as a plurality may be implemented as singular instances of such features. The drawings are intended to be illustrative and may not precisely depict some implementations. Variations in sizing, placement, shapes, angles, and/or the positioning of features relative to each other are possible.

[0274] For the avoidance of any doubt all variations and modifications discussed in the above paragraph are only possible to the extent that they fall within the scope of the appended claims.

Claims

1. A computer-implemented method for providing personal security features to a user of a mobile computing device (102), the method comprising: receiving, at the mobile computing device(102), input (120) from the user (110) of the mobile computing device (102) that indicates a safety incident is occurring that poses a potential threat (112) to the user's personal safety;

determining a location of the mobile computing device (102) using one or more of a plurality of data sources;

receiving information that indicates whether responders (116a; 116b; 116c; 116d) are currently available for the user of the mobile computing device (102);

if it is detected that no responders are currently available, taking an appropriate alternate action; communicating, by the mobile computing device(102), with another computing device (108a; 108b; 108c; 108d) as part of a two-way video chat session (126) over a first network connection, the communicating including transmitting

the location of the mobile computing device(124); and displaying (142), as part of the two-way video chat session, real-time video (140) from the other computing device wherein the real-time video (140) is output by the mobile computing device (102) in a manner to convey (152) to one or more people involved in the safety incident (112; 110) that a remote user (116a; 116b; 116c; 116d) of the other computing device (108a; 108b; 108c; 108d) is observing the incident in real time; recording video of the safety incident using one or more cameras that are accessible to the mobile computing device (102); and transmitting, concurrently while displaying the real-time video and over a second network connection, the video of the safety incident to a remote storage system (106) for persistent storage.

2. The computer-implemented method of claim 1, further comprising:

identifying from a data source a plurality of potential responder computing devices (108a; 108b; 108c; 108d) that are used by candidate responders (116a; 116b; 116c; 116d); and automatically selecting a particular potential responder computing device (108a; 108b; 108c; 108d) to communicate with that is used by a particular potential candidate responder (116a; 116b; 116c; 116d) based, at least in part, on one or more factors including status information that indicates whether the responder is currently available to communicate with the user.

3. The computer-implemented method of claim 1, further comprising:

receiving, at the mobile computing device (102), a location of a responder through a network connection (104); and displaying the location of the responder on the mobile computing device.

4. The computer-implemented method of claim 1, further comprising:

establishing, before initiating the communication session at the other computing device, network connections with a plurality of other devices (108a; 108b; 108c; 108d) that are used by candidate responders (116a; 116b; 116c; 116d); and

obtaining and displaying, using the network connections, current status information for a plurality of candidate responders.

5. The computer-implemented method of claim 1, further comprising:

receiving, at the mobile computing device (102) and from a responder computing device (108a; 108b; 108c; 108d), instructions to perform one or more operations;

checking permission on the mobile computing device to determine whether the responder computing device (108a; 108b; 108c; 108d) has permission to remotely control operation of the mobile computing device (102); and

if the responder computing device has permission to remotely control operation of the mobile computing device (102) based on the determining, performing, the one or more operations.

6. The computer-implemented method of claim 1, further comprising:

encrypting, by the mobile computing device, real-time data with metadata that identifies when, where, or by whom the real-time data was collected; and
transmitting the real-time data (124).

7. The computer-implemented method of claim 1, further comprising:

receiving a current location for a user (110); and
determining a current safety level for the user (110) at the current location based on one or more factors including the location.

8. The computer-implemented method of claim 1, wherein a communication protocol that is used comprises webRTC.

9. A computing device comprising:

a user interface that is programmed to receive input (120) from a user (110) of the computing device (102) that indicates a safety incident that poses a potential threat to personal safety and to receive information that indicates whether responders are currently available for a user of the computing device;

one or more cameras that are programmed to record video of the safety incident;

a geographic location unit that is programmed to determine a location of a computing device using one or more of a plurality of data sources; a network interface that is programmed to communicate with another computing device (108a; 108b; 108c; 108d) as part of a two-way video chat session over a first network connection (126) and to cause the video of the safety incident to be concurrently transmitted (128), over

a second network connection, to a remote storage system (106) for persistent storage, the location of the computing device being sent over the first and second network connections, wherein the network interface is further programmed to take appropriate alternate action if it is detected that no responders are currently available; and

a display (142) that is programmed to display, as part of the two-way video chat session, real-time video from the other computing device, wherein the real-time video is output by the display in a manner to convey to one or more people involved in the safety incident (112; 110) that a remote user (116a; 116b; 116c; 116d) of the other computing device (108a; 108b; 108c; 108d) is observing the incident in real time.

10. The computing device of claim 9, further comprising: a security application that is programmed to identify a plurality of candidate responders (116a; 116b; 116c; 116d) and to select a particular candidate responder (116a; 116b; 116c; 116d) based, at least in part, on one or more factors, wherein the particular candidate responder (116a; 116b; 116c; 116d) is associated with the other computing device (108a; 108b; 108c; 108d).

11. The computing device of claim 9, wherein the network interface is further programmed to establish (114), before initiating the communication with the other computing device, network connections with a plurality of other computing devices associated with candidate responders (116a; 116b; 116c; 116d); wherein the device further comprises:

a status module that is programmed to obtain, using the network connections, current status information for a plurality of candidate responders; and

wherein the display is programmed to display the current status information for a plurality of candidate responders.

12. The computer-implemented method of claim 2, further comprising: determining, using a database of locations and corresponding licensure status, whether the user (110) is located within one or more licensed jurisdictions.

Patentansprüche

1. Computerimplementiertes Verfahren zum Bereitstellen von persönlichen Sicherheitsmerkmalen für einen Benutzer einer mobilen Computervorrichtung (102), wobei das Verfahren umfasst:

in der mobilen Computervorrichtung (102) erfolgreiches Empfangen einer Eingabe (120) von dem Benutzer (110) der mobilen Computervorrichtung (102), die angibt, dass ein Sicherheitsvorfall auftritt, der eine potenzielle Bedrohung (112) für die persönliche Sicherheit des Benutzers darstellt;

Bestimmen eines Standorts der mobilen Computervorrichtung (102) unter Verwendung von einer oder mehreren aus einer Vielzahl von Datenquellen;

Empfangen von Information, die angibt, ob derzeit Helfer (116a; 116b; 116c; 116d) für den Benutzer der mobilen Computervorrichtung (102) verfügbar sind;

wenn ermittelt wird, dass derzeit keine Helfer verfügbar sind, Ergreifen einer geeigneten alternativen Maßnahme;

Kommunizieren durch die mobile Computervorrichtung (102) mit einer anderen Computervorrichtung (108a; 108b; 108c; 108d) als Teil einer Zweiwege-Videochatsitzung (126) über eine erste Netzwerkverbindung, wobei das Kommunizieren einschließt: Übertragen des Standorts von der mobilen Computervorrichtung (124); und

Anzeigen (142) eines Echtzeitvideos (140) von der anderen Computervorrichtung als Teil der Zweiwege-Videochatsitzung, worin das Echtzeitvideo (140) durch die mobile Computervorrichtung (102) auf eine Weise ausgegeben wird, dass einer oder mehreren an dem Sicherheitsvorfall beteiligten Personen (112; 110) mitgeteilt (152) wird, dass ein entfernter Benutzer (116a; 116b; 116c; 116d) der anderen Computervorrichtung (108a; 108b; 108c; 108d) den Vorfall in Echtzeit beobachtet;

Aufzeichnen eines Videos des Sicherheitsvorfalls unter Verwendung einer oder mehrerer Kameras, die für die mobile Computervorrichtung (102) zugänglich sind; und

gleichzeitig mit dem Anzeigen des Echtzeitvideos und über eine zweite Netzwerkverbindung erfolgreiches Übertragen des Videos des Sicherheitsvorfalls zu einem entfernten Speichersystem (106) zwecks dauerhafter Speicherung.

2. Computerimplementiertes Verfahren nach Anspruch 1, ferner umfassend:

Identifizieren einer Vielzahl von potenziellen Helfer-Computervorrichtungen (108a; 108b; 108c; 108d), die durch Helferkandidaten (116a; 116b; 116c; 116d) verwendet werden, aus einer Datenquelle; und

automatisches Auswählen einer bestimmten potenziellen Helfer-Computervorrichtung (108a; 108b; 108c; 108d), mit der zu kommuni-

zieren ist, die durch einen bestimmten potenziellen Helferkandidaten (116a; 116b; 116c; 116d) verwendet wird, und zwar zumindest teilweise auf der Grundlage von einem oder mehreren Faktoren, einschließlich Statusinformation, die angibt, ob der Helfer aktuell verfügbar ist, um mit dem Benutzer zu kommunizieren.

3. Computerimplementiertes Verfahren nach Anspruch 1, ferner umfassend:

in der mobilen Computervorrichtung (102) erfolgreiches Empfangen eines Standorts eines Helfers über eine Netzwerkverbindung (104); und Anzeigen des Standorts des Helfers auf der mobilen Computervorrichtung.

4. Computerimplementiertes Verfahren nach Anspruch 1, ferner umfassend:

vor dem Einleiten der Kommunikationssitzung in der anderen Computervorrichtung erfolgreiches Aufbauen von Netzwerkverbindungen mit einer Vielzahl von anderen Vorrichtungen (108a; 108b; 108c; 108d), die durch Helferkandidaten (116a; 116b; 116c; 116d) verwendet werden; und

Erlangen und Anzeigen von aktueller Statusinformation für eine Vielzahl von Helferkandidaten unter Verwendung der Netzwerkverbindungen.

5. Computerimplementiertes Verfahren nach Anspruch 1, ferner umfassend:

in der mobilen Computervorrichtung (102) und von einer Helfer-Computervorrichtung (108a; 108b; 108c; 108d) erfolgreiches Empfangen von Anweisungen, eine oder mehrere Operationen durchzuführen;

Prüfen der Erlaubnis auf der mobilen Computervorrichtung, um zu bestimmen, ob die Helfer-Computervorrichtung (108a; 108b; 108c; 108d) die Erlaubnis hat, den Betrieb der mobilen Computervorrichtung (102) fernzusteuern; und wenn die Helfer-Computervorrichtung aufgrund des Bestimmens die Erlaubnis hat, den Betrieb der mobilen Computervorrichtung (102) fernzusteuern, Durchführen der einen oder mehreren Operationen.

6. Computerimplementiertes Verfahren nach Anspruch 1, ferner umfassend:

durch die mobile Computervorrichtung erfolgreiches Verschlüsseln von Echtzeitdaten mit Metadaten, die angeben, wann, wo oder durch wen die Echtzeitdaten gesammelt wurden; und Übertragen der Echtzeitdaten (124).

7. Computerimplementiertes Verfahren nach Anspruch 1, ferner umfassend:
- Empfangen eines aktuellen Standorts für einen Benutzer (110); und
Bestimmen eines aktuellen Sicherheitsniveaus für den Benutzer (110) am aktuellen Standort auf der Grundlage von einem oder mehreren Faktoren einschließlich des Standorts.
8. Computerimplementiertes Verfahren nach Anspruch 1, worin ein Kommunikationsprotokoll, das verwendet wird, WebRTC umfasst.
9. Computervorrichtung, umfassend:
- eine Benutzerschnittstelle, die dafür programmiert ist, eine Eingabe (120) von einem Benutzer (110) der Computervorrichtung (102) zu empfangen, die einen Sicherheitsvorfall angibt, der eine potenzielle Bedrohung für die persönliche Sicherheit darstellt, und Information zu empfangen, die angibt, ob derzeit Helfer für einen Benutzer der Computervorrichtung verfügbar sind;
- eine oder mehrere Kameras, die dafür programmiert sind, ein Video des Sicherheitsvorfalls aufzuzeichnen;
- eine Einheit für den geografischen Standort, die dafür programmiert ist, einen Standort einer Computervorrichtung unter Verwendung von einer oder mehreren aus einer Vielzahl von Datenquellen zu bestimmen;
- eine Netzwerkschnittstelle, die dafür programmiert ist, mit einer anderen Computervorrichtung (108a; 108b; 108c; 108d) als Teil einer Zweiwege-Videochatsitzung über eine erste Netzwerkverbindung (126) zu kommunizieren und zu veranlassen, dass gleichzeitig über eine zweite Netzwerkverbindung das Video des Sicherheitsvorfalls zwecks dauerhafter Speicherung zu einem entfernten Speichersystem (106) übertragen (128) wird, wobei der Standort der Computervorrichtung über die erste und die zweite Netzwerkverbindung gesendet wird, worin die Netzwerkschnittstelle ferner dafür programmiert ist, geeignete alternative Maßnahmen zu ergreifen, wenn ermittelt wird, dass derzeit keine Helfer verfügbar sind; und
- eine Anzeige (142), die dafür programmiert ist, als Teil der Zweiwege-Videochatsitzung ein Echtzeitvideo von der anderen Computervorrichtung anzuzeigen, worin das Echtzeitvideo durch die Anzeige auf eine Weise ausgegeben wird, dass einer oder mehreren an dem Sicherheitsvorfall beteiligten Personen (112; 110) mitgeteilt wird, dass ein entfernter Benutzer (116a; 116b; 116c; 116d) der anderen Computervor-
- richtung (108a; 108b; 108c; 108d) den Vorfall in Echtzeit beobachtet.
10. Computervorrichtung nach Anspruch 9, ferner umfassend:
- eine Sicherheitsanwendung, die dafür programmiert ist, eine Vielzahl von Helferkandidaten (116a; 116b; 116c; 116d) zu identifizieren und einen bestimmten Helferkandidaten (116a; 116b; 116c; 116d) zumindest teilweise auf der Grundlage von einem oder mehreren Faktoren auszuwählen, worin der bestimmte Helferkandidat (116a; 116b; 116c; 116d) der anderen Computervorrichtung (108a; 108b; 108c; 108d) zugeordnet ist.
11. Computervorrichtung nach Anspruch 9, worin die Netzwerkschnittstelle ferner dafür programmiert ist, vor dem Einleiten der Kommunikation mit der anderen Computervorrichtung Netzwerkverbindungen mit einer Vielzahl von anderen Computervorrichtungen, die Helferkandidaten (116a; 116b; 116c; 116d) zugeordnet sind, aufzubauen (114); worin die Vorrichtung ferner umfasst:
- ein Statusmodul, das dafür programmiert ist, unter Verwendung der Netzwerkverbindungen aktuelle Statusinformation für eine Vielzahl von Helferkandidaten zu erlangen; und
- worin die Anzeige dafür programmiert ist, die aktuelle Statusinformation für eine Vielzahl von Helferkandidaten anzuzeigen.
12. Computerimplementiertes Verfahren nach Anspruch 2, ferner umfassend:
- unter Verwendung einer Datenbank von Standorten und entsprechenden Zulassungsstatus erfolgreiches Bestimmen, ob sich der Benutzer (110) innerhalb von einem oder mehreren lizenzierten Zuständigkeitsbereichen befindet.
- Revendications**
1. Procédé mis en oeuvre par ordinateur pour fournir des caractéristiques de sécurité personnelle à un utilisateur d'un dispositif informatique mobile (102), le procédé comprenant :
- la réception, au niveau du dispositif informatique mobile (102), d'une entrée (120) en provenance de l'utilisateur (110) du dispositif informatique mobile (102) qui indique qu'un incident de sécurité qui constitue une menace potentielle (112) pour la sécurité personnelle de l'utilisateur est en train de survenir ;
- la détermination d'une localisation du dispositif informatique mobile (102) en utilisant une ou plusieurs d'une pluralité de sources de

données ;

la réception d'une information qui indique si oui ou non des répondeurs (116a ; 116b ; 116c ; 116d) sont présentement disponibles pour l'utilisateur du dispositif informatique mobile (102) ; s'il est détecté qu'aucun répondeur n'est présentement disponible, la réalisation d'une action alternative appropriée ;

la réalisation d'une communication, par le dispositif informatique mobile (102), avec un autre dispositif informatique (108a ; 108b ; 108c ; 108d) en tant que partie d'une session de conversation en ligne vidéo bidirectionnelle (126) sur une première connexion de réseau, la communication incluant la transmission de la localisation du dispositif informatique mobile (124) ; et

l'affichage (142), en tant que partie de la session de conversation en ligne vidéo bidirectionnelle, d'une vidéo en temps réel (140) en provenance de l'autre dispositif informatique, dans lequel la vidéo en temps réel (140) est émise en sortie par le dispositif informatique mobile (102) de manière à convoier (152) jusqu'à une ou plusieurs personne(s) mise(s) en jeu dans l'incident de sécurité (112 ; 110) le fait qu'un utilisateur à distance (116a ; 116b ; 116c ; 116d) de l'autre dispositif informatique (108a ; 108b ; 108c ; 108d) est en train d'observer l'incident en temps réel ;

l'enregistrement d'une vidéo de l'incident de sécurité en utilisant une ou plusieurs caméra(s) qui est/sont accessible(s) pour le dispositif informatique mobile (102) ; et

la transmission, concurrentement à l'affichage de la vidéo en temps réel et sur une seconde connexion de réseau, de la vidéo de l'incident de sécurité à un système de stockage à distance (106) en vue d'un stockage persistant.

2. Procédé mis en oeuvre par ordinateur selon la revendication 1, comprenant en outre :

l'identification, à partir d'une source de données, d'une pluralité de dispositifs informatiques de répondeur potentiel (108a ; 108b ; 108c ; 108d) qui sont utilisés par des répondeurs candidats (116a ; 116b ; 116c ; 116d) ; et

la sélection automatique d'un dispositif informatique de répondeur potentiel particulier (108a ; 108b ; 108c ; 108d) pour communiquer avec, lequel est utilisé par un répondeur candidat potentiel (116a ; 116b ; 116c ; 116d) sur la base, au moins en partie, d'un ou de plusieurs facteur(s) incluant une information d'état qui indique si oui ou non le répondeur est présentement disponible pour communiquer avec l'utilisateur.

3. Procédé mis en oeuvre par ordinateur selon la revendication 1, comprenant en outre :

la réception, au niveau du dispositif informatique mobile (102), d'une localisation d'un répondeur par l'intermédiaire d'une connexion de réseau (104) ; et

l'affichage de la localisation du répondeur sur le dispositif informatique mobile.

4. Procédé mis en oeuvre par ordinateur selon la revendication 1, comprenant en outre :

l'établissement, avant l'initiation de la session de communication au niveau de l'autre dispositif informatique, de connexions de réseau avec une pluralité d'autres dispositifs (108a ; 108b ; 108c ; 108d) qui sont utilisés par des répondeurs candidats (116a ; 116b ; 116c ; 116d) ; et

l'obtention et l'affichage, en utilisant les connexions de réseau, d'une information d'état courant pour une pluralité de répondeurs candidats.

5. Procédé mis en oeuvre par ordinateur selon la revendication 1, comprenant en outre :

la réception, au niveau du dispositif informatique mobile (102) et en provenance d'un dispositif informatique de répondeur (108a ; 108b ; 108c ; 108d), d'instructions pour réaliser une ou plusieurs opération(s) ;

la vérification de l'autorisation sur le dispositif informatique mobile afin de déterminer si oui ou non le dispositif informatique de répondeur (108a ; 108b ; 108c ; 108d) dispose de l'autorisation de commander à distance le fonctionnement du dispositif informatique mobile (102) ; et si le dispositif informatique de répondeur dispose de l'autorisation de commander à distance le fonctionnement du dispositif informatique mobile (102) sur la base de la détermination, la réalisation des une ou plusieurs opérations.

6. Procédé mis en oeuvre par ordinateur selon la revendication 1, comprenant en outre :

le cryptage, par le dispositif informatique mobile, de données en temps réel à l'aide de métadonnées qui identifient lorsque, où ou par qui les données en temps réel ont été collectées ; et la transmission des données en temps réel (124).

7. Procédé mis en oeuvre par ordinateur selon la revendication 1, comprenant en outre :

la réception d'une localisation courante pour un utilisateur (110) ; et

la détermination d'un niveau de sécurité courant pour l'utilisateur (110) au niveau de la localisation courante sur la base d'un ou de plusieurs facteur(s) incluant la localisation.

8. Procédé mis en oeuvre par ordinateur selon la revendication 1, dans lequel un protocole de communication qui est utilisé comprend webRTC.

9. Dispositif informatique comprenant :

une interface utilisateur qui est programmée de manière à ce qu'elle reçoive une entrée (120) en provenance d'un utilisateur (110) du dispositif informatique (102) qui indique un incident de sécurité qui constitue une menace potentielle pour la sécurité personnelle et de manière à ce qu'elle reçoive une information qui indique si oui ou non des répondeurs sont présentement disponibles pour un utilisateur du dispositif informatique ;

une ou plusieurs caméra(s) qui est/sont programmée(s) de manière à ce qu'elle(s) enregistre(nt) une vidéo de l'incident de sécurité ;

une unité de localisation géographique qui est programmée de manière à ce qu'elle détermine une localisation d'un dispositif informatique en utilisant une ou plusieurs d'une pluralité de sources de données ;

une interface de réseau qui est programmée de manière à ce qu'elle communique avec un autre dispositif informatique (108a ; 108b ; 108c ; 108d) en tant que partie d'une session de conversation en ligne vidéo bidirectionnelle sur une première connexion de réseau (126) et de manière à ce qu'elle ait pour effet que la vidéo de l'incident de sécurité soit transmise concurrentement (128), sur une seconde connexion de réseau, jusqu'à un système de stockage à distance (106) en vue d'un stockage persistant, la localisation du dispositif informatique étant envoyée sur les première et seconde connexions de réseau, dans lequel l'interface de réseau est en outre programmée de manière à ce qu'elle réalise une action alternative appropriée s'il est détecté qu'aucun répondeur n'est présentement disponible ; et

un affichage (142) qui est programmé de manière à ce qu'il affiche, en tant que partie de la session de conversation en ligne vidéo bidirectionnelle, une vidéo en temps réel en provenance de l'autre dispositif informatique, dans lequel la vidéo en temps réel est émise en sortie par l'affichage de manière à convoier jusqu'à une ou plusieurs personne(s) mise(s) en jeu dans l'incident de sécurité (112 ; 110) le fait qu'un utilisateur à distance (116a ; 116b ; 116c ; 116d) de l'autre dispositif informatique (108a ; 108b ;

108c ; 108d) est en train d'observer l'incident en temps réel.

10. Dispositif informatique selon la revendication 9, comprenant en outre :

une application de sécurité qui est programmée de manière à ce qu'elle identifie une pluralité de répondeurs candidats (116a ; 116b ; 116c ; 116d) et de manière à ce qu'elle sélectionne un répondeur candidat particulier (116a ; 116b ; 116c ; 116d) sur la base, au moins en partie, d'un ou de plusieurs facteur(s), dans lequel le répondeur candidat particulier (116a ; 116b ; 116c ; 116d) est associé à l'autre dispositif informatique (108a ; 108b ; 108c ; 108d).

11. Dispositif informatique selon la revendication 9, dans lequel l'interface de réseau est en outre programmée de manière à ce qu'elle établisse (114), avant l'initiation de la communication avec l'autre dispositif informatique, des connexions de réseau avec une pluralité d'autres dispositifs informatiques qui sont associés à des répondeurs candidats (116a ; 116b ; 116c ; 116d) ; dans lequel le dispositif comprend en outre :

un module d'état qui est programmé de manière à ce qu'il obtienne, en utilisant les connexions de réseau, une information d'état courant pour une pluralité de répondeurs candidats ; et dans lequel : l'affichage est programmé de manière à ce qu'il affiche l'information d'état courant pour une pluralité de répondeurs candidats.

12. Procédé mis en oeuvre par ordinateur selon la revendication 2, comprenant en outre :

la détermination, en utilisant une base de données de localisations et un état d'autorisation par licence correspondant, si oui ou non l'utilisateur (110) est localisé à l'intérieur d'un ou de plusieurs territoire(s) ayant fait l'objet d'une autorisation par licence.

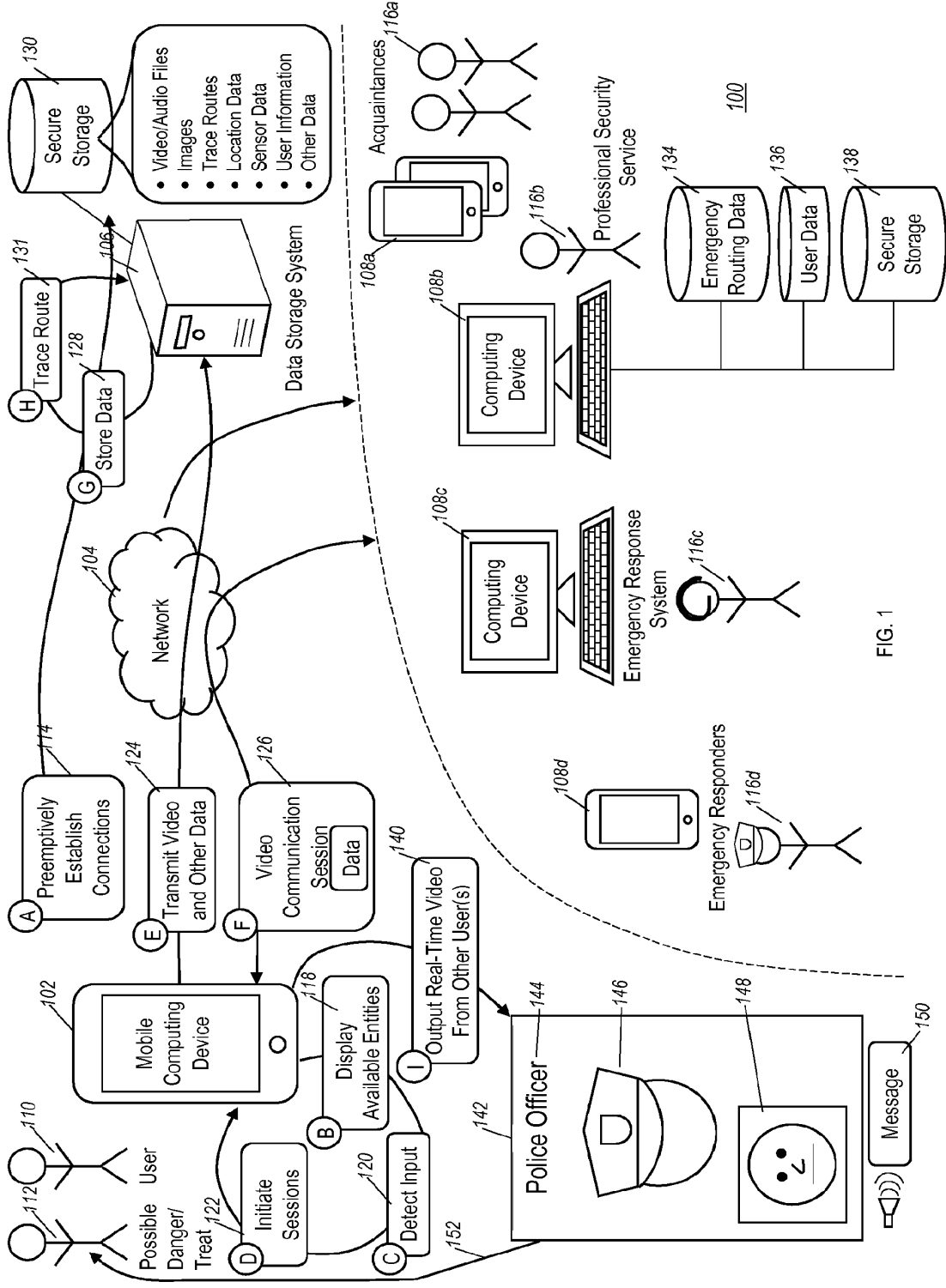


FIG. 1

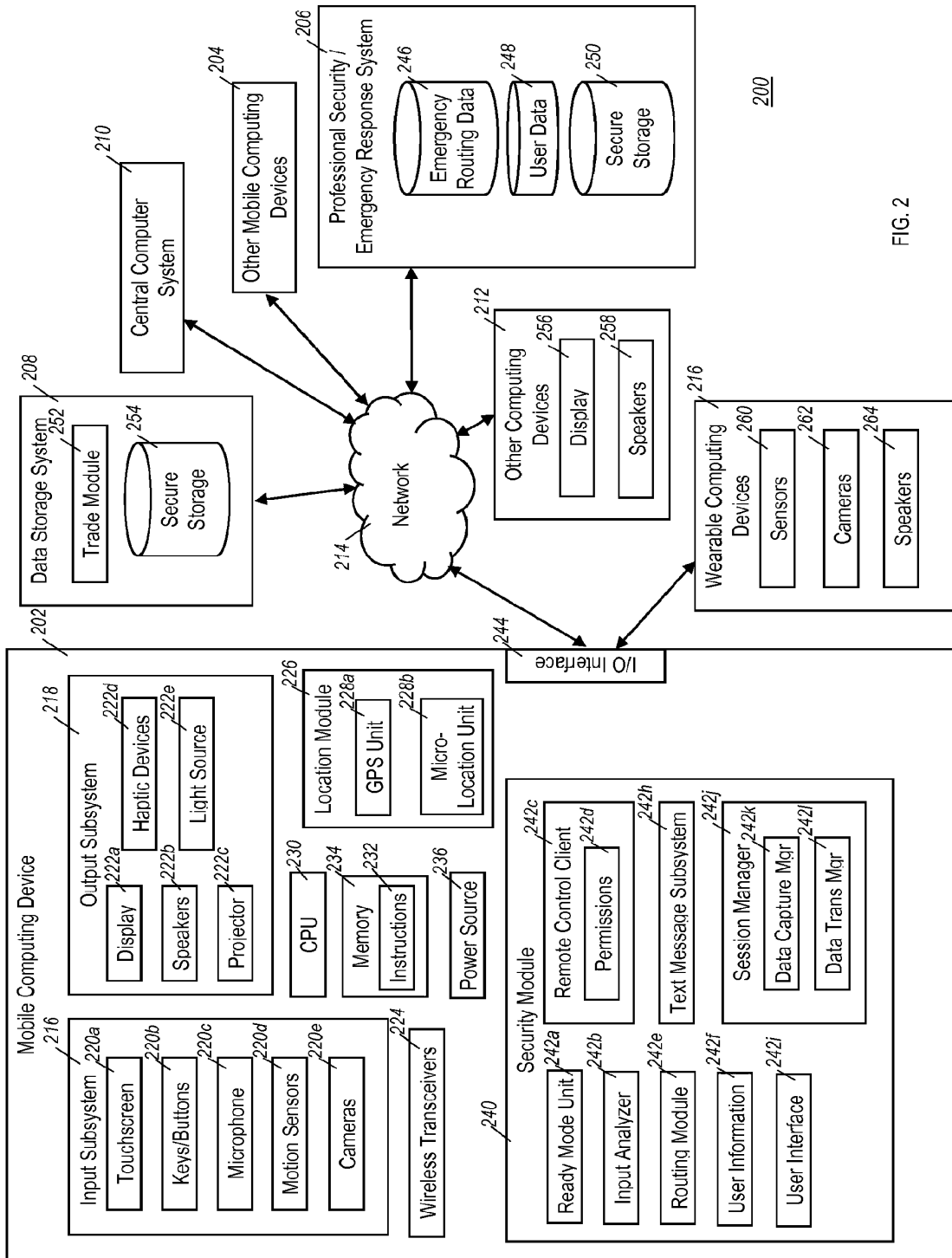


FIG. 2

300

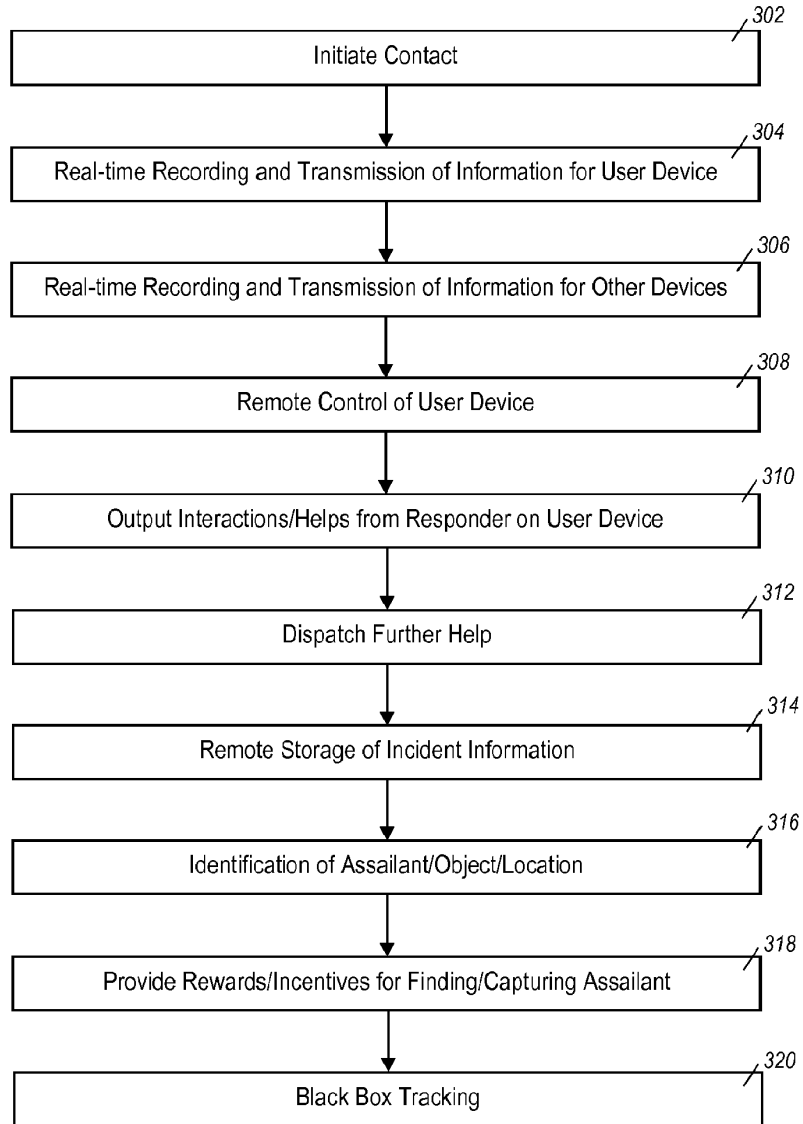


FIG. 3

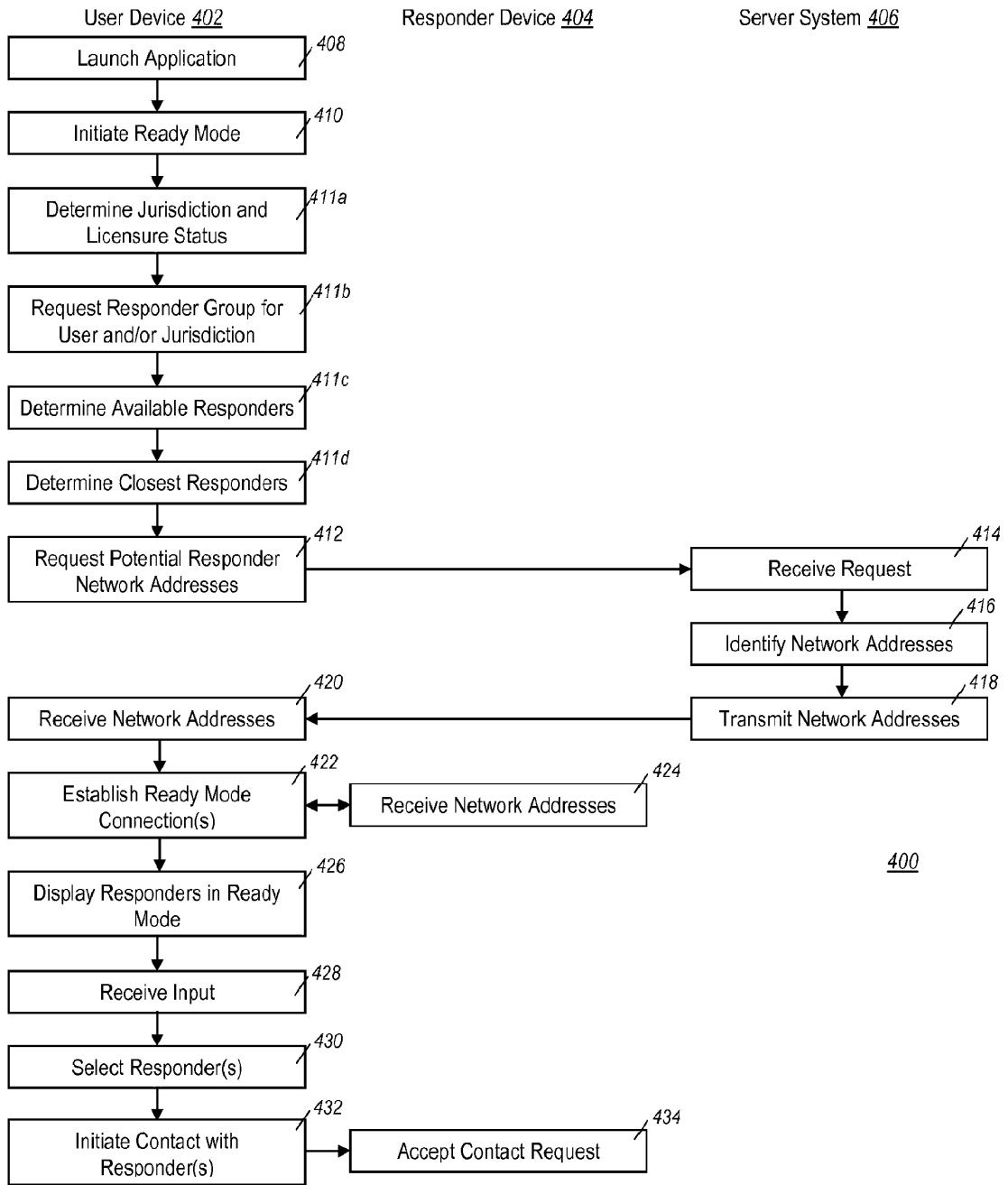


FIG. 4

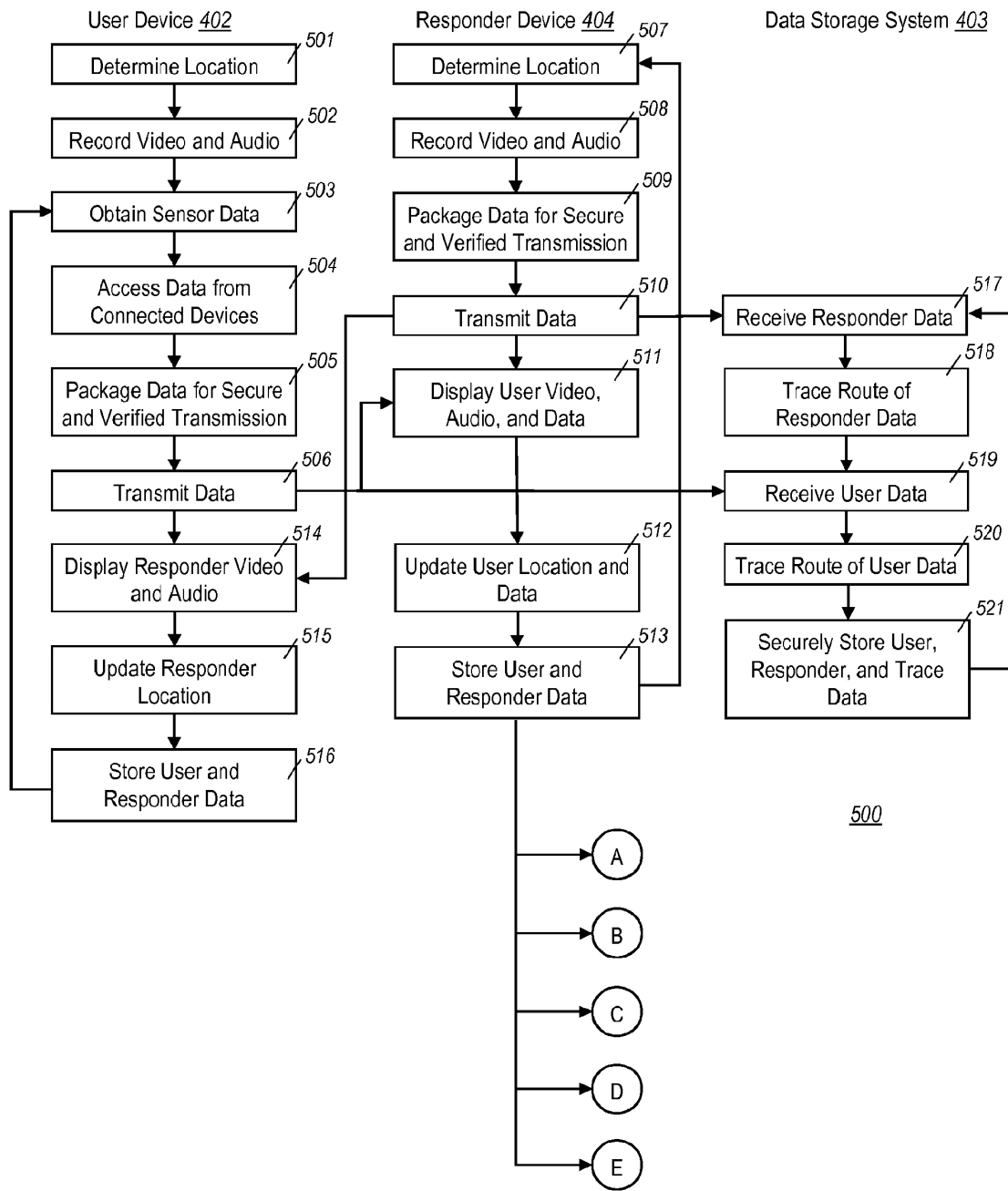


FIG. 5A

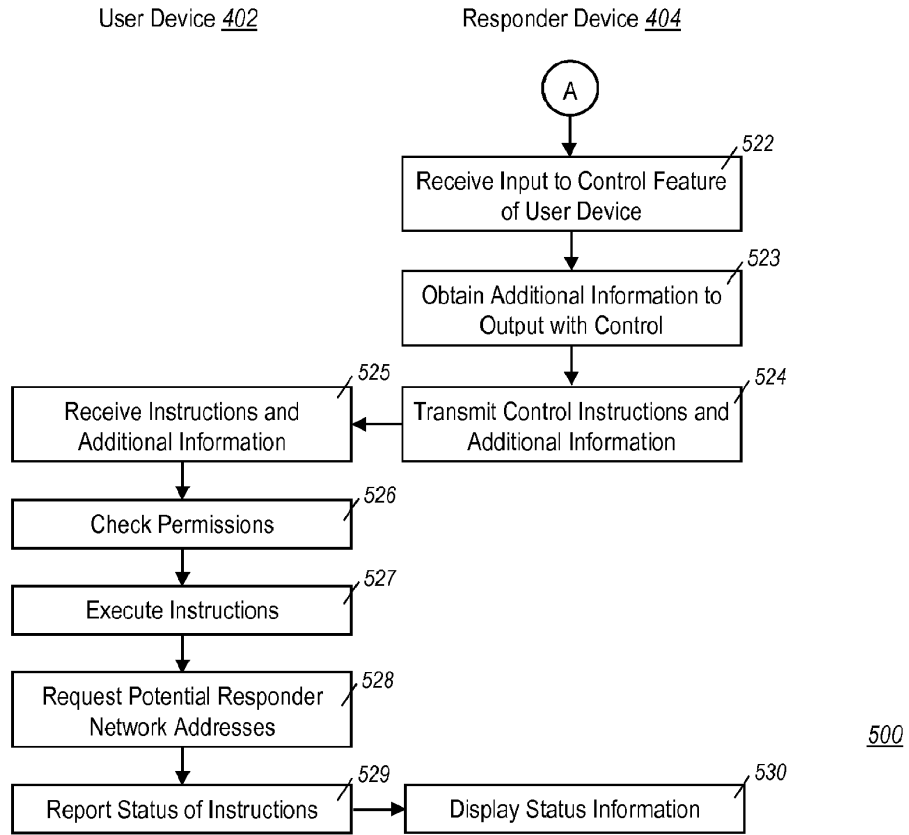
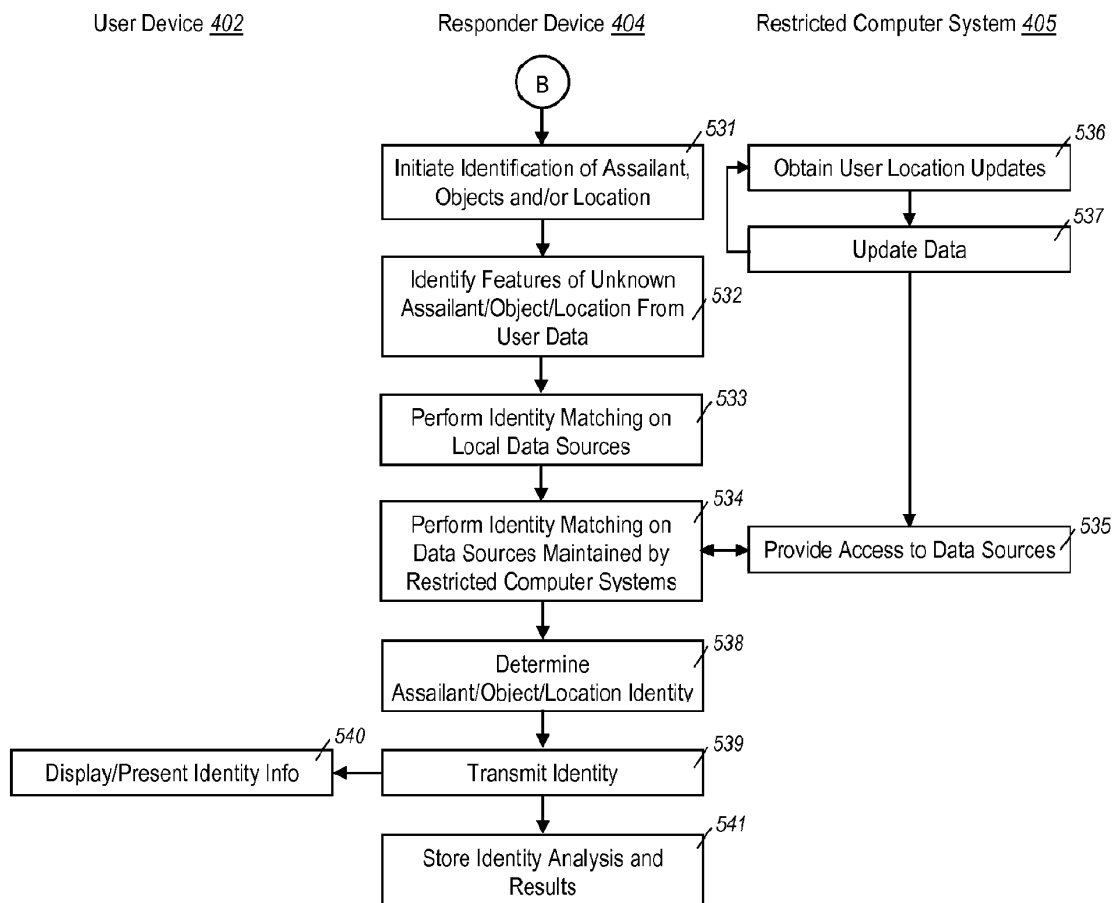
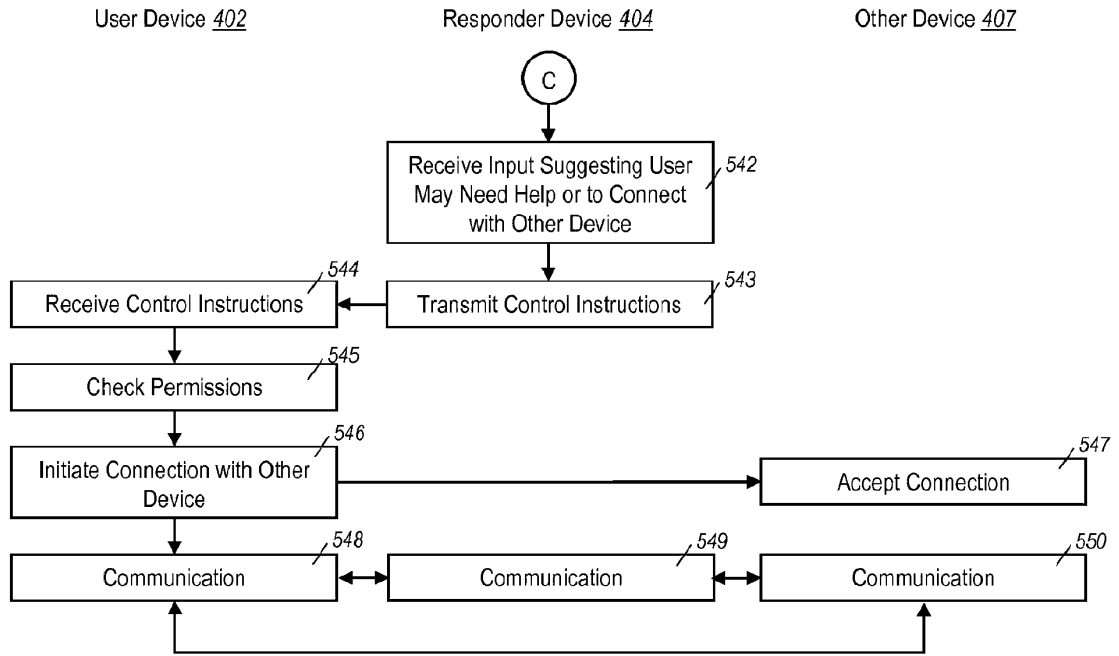


FIG. 5B



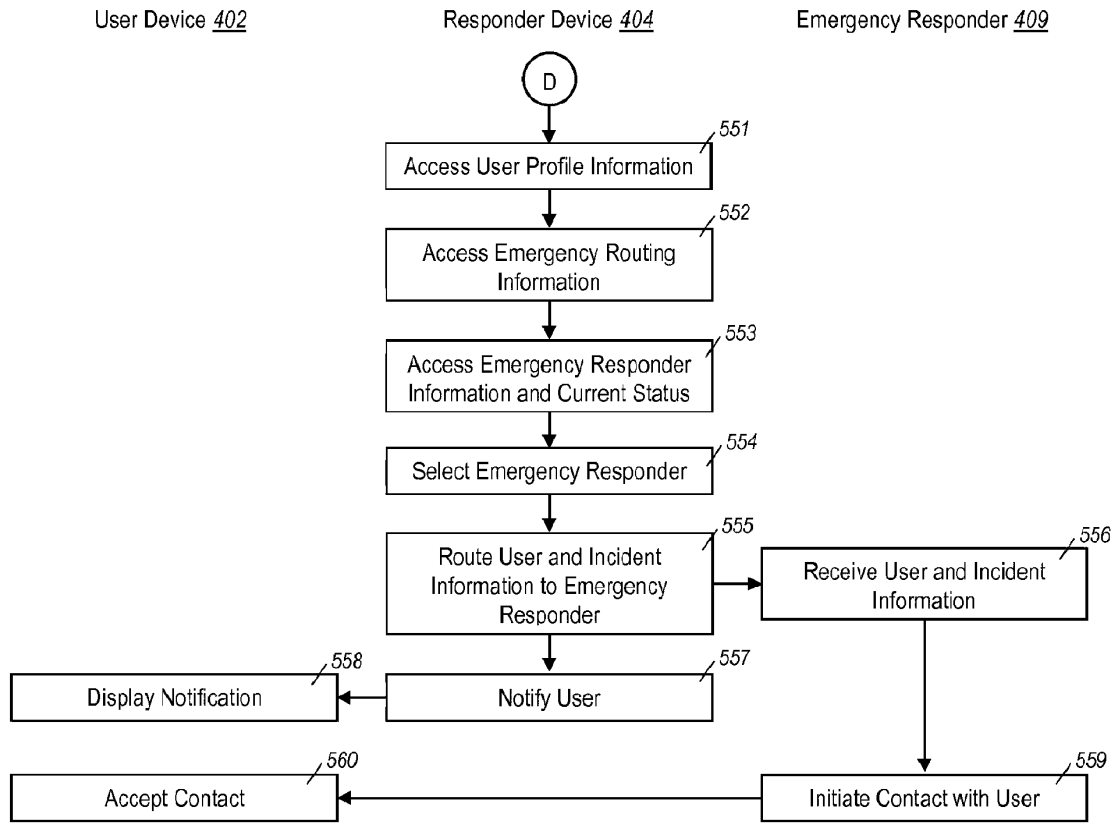
500

FIG. 5C



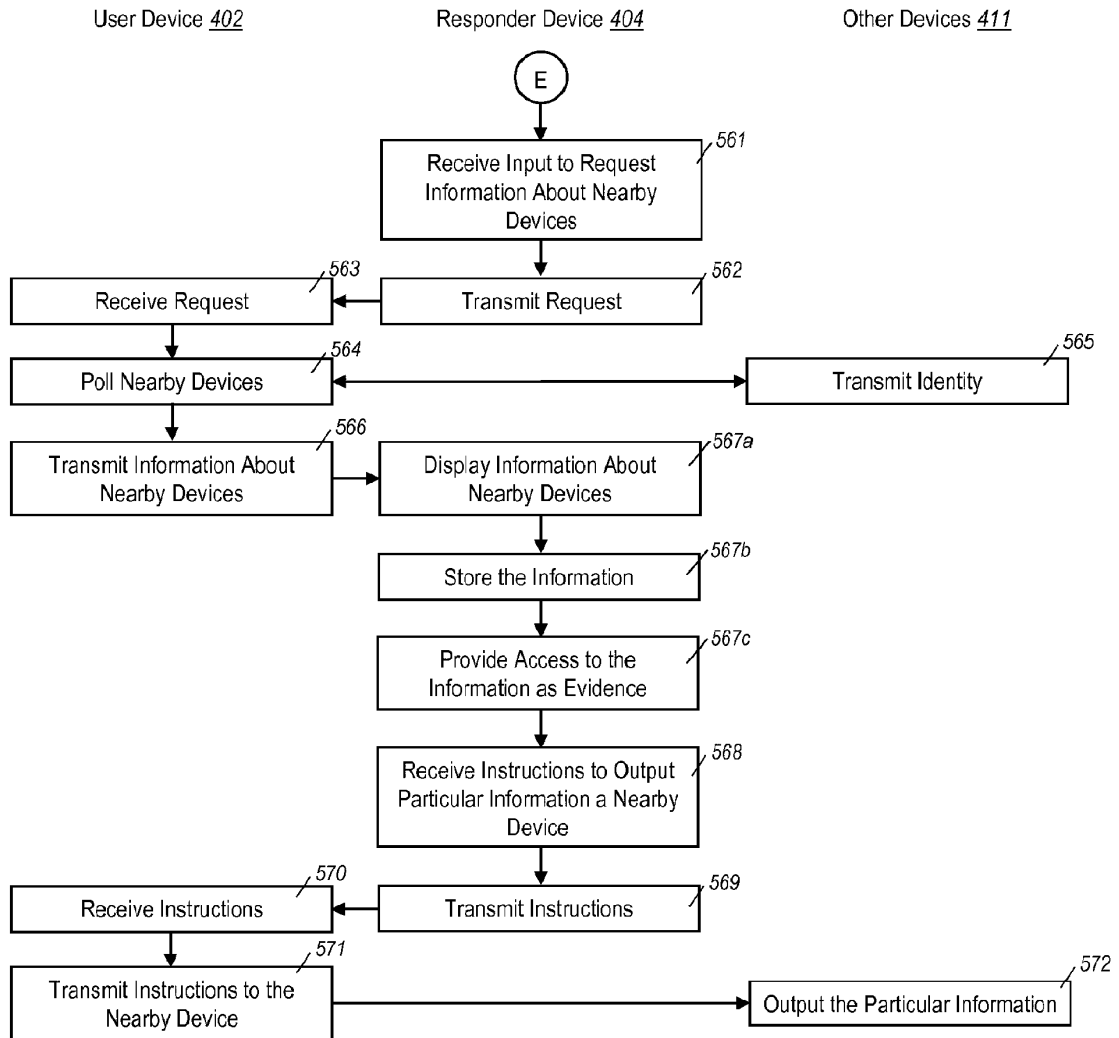
500

FIG. 5D



500

FIG. 5E



500

FIG. 5F

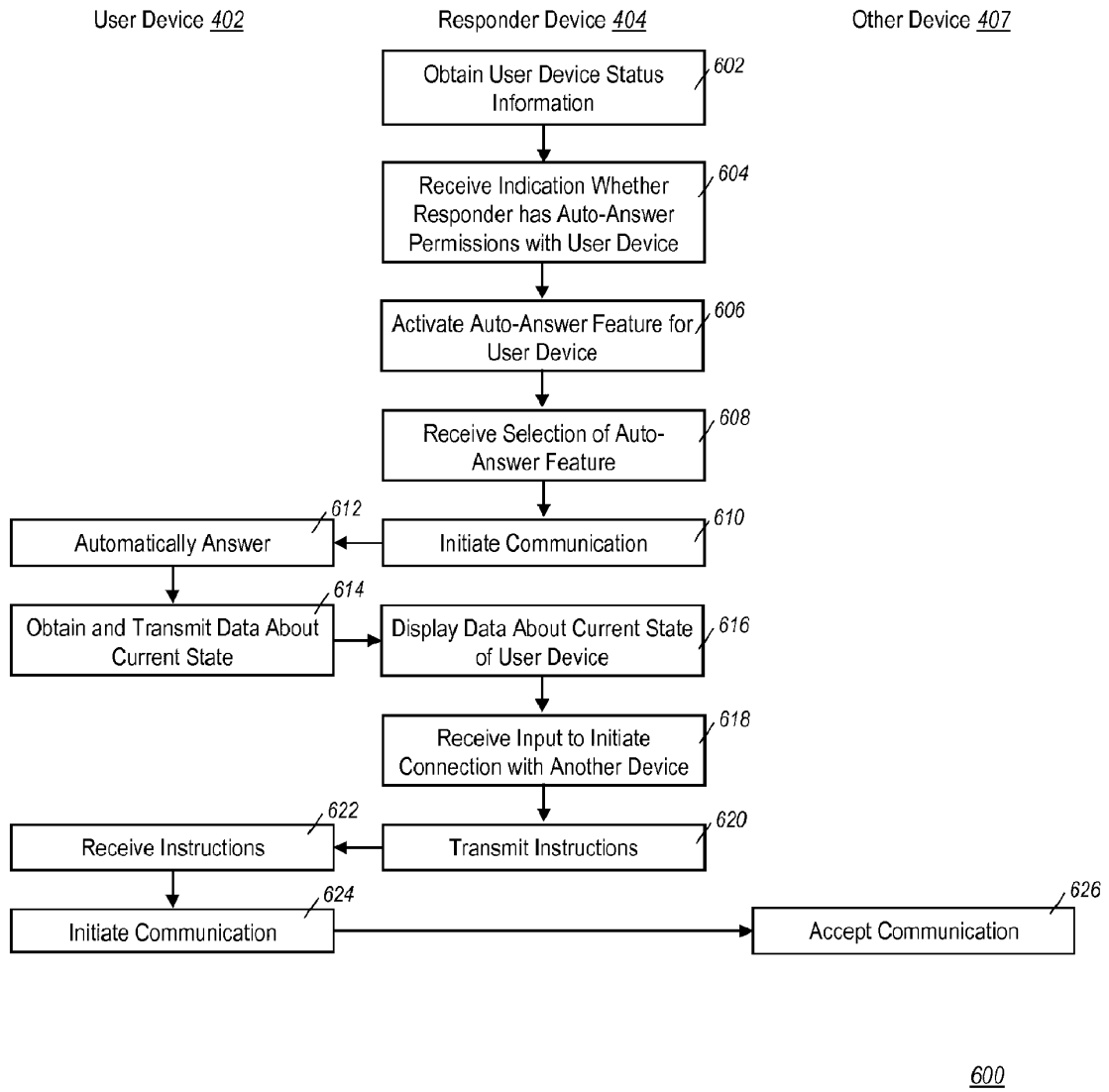


FIG. 6

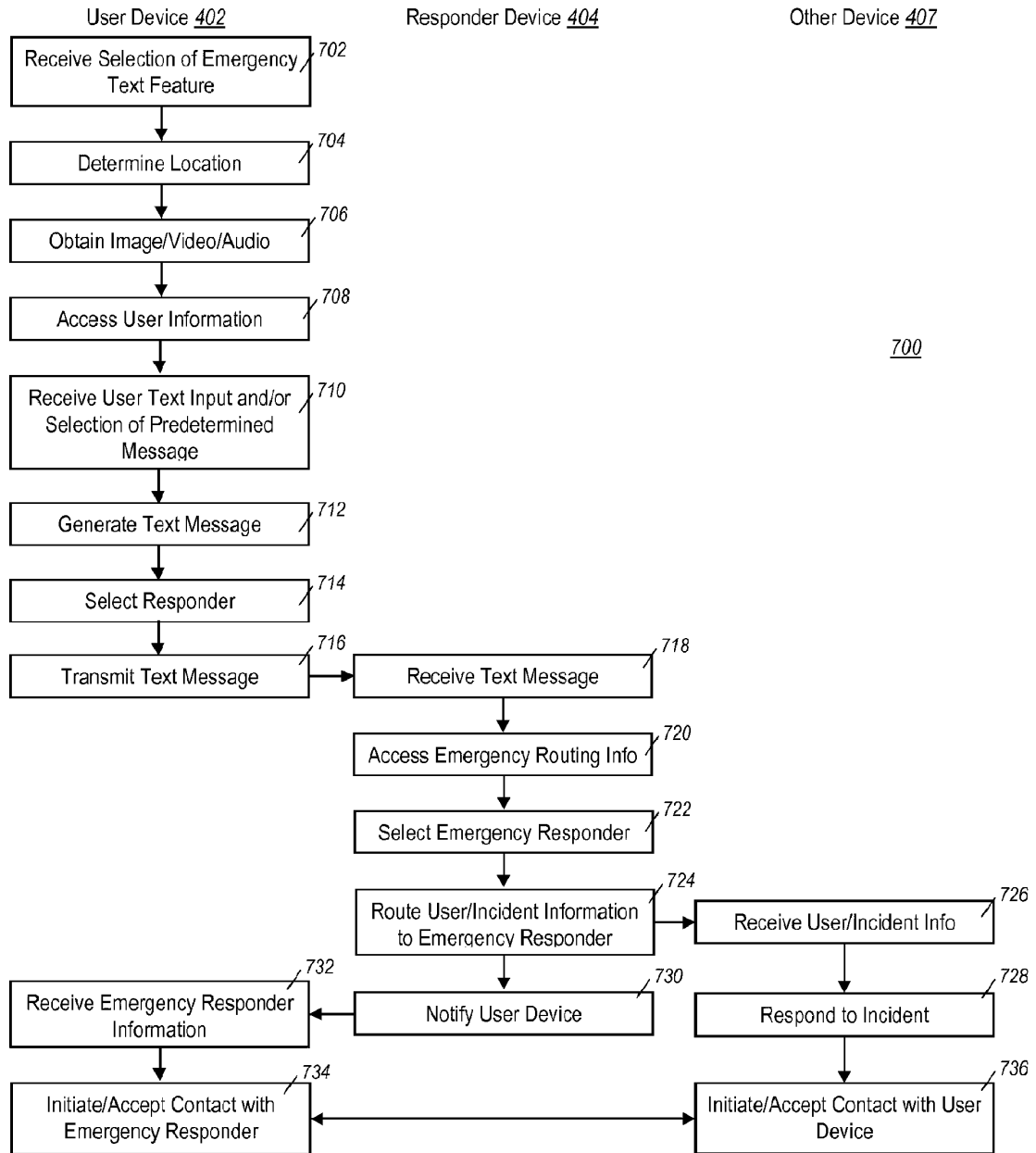


FIG. 7

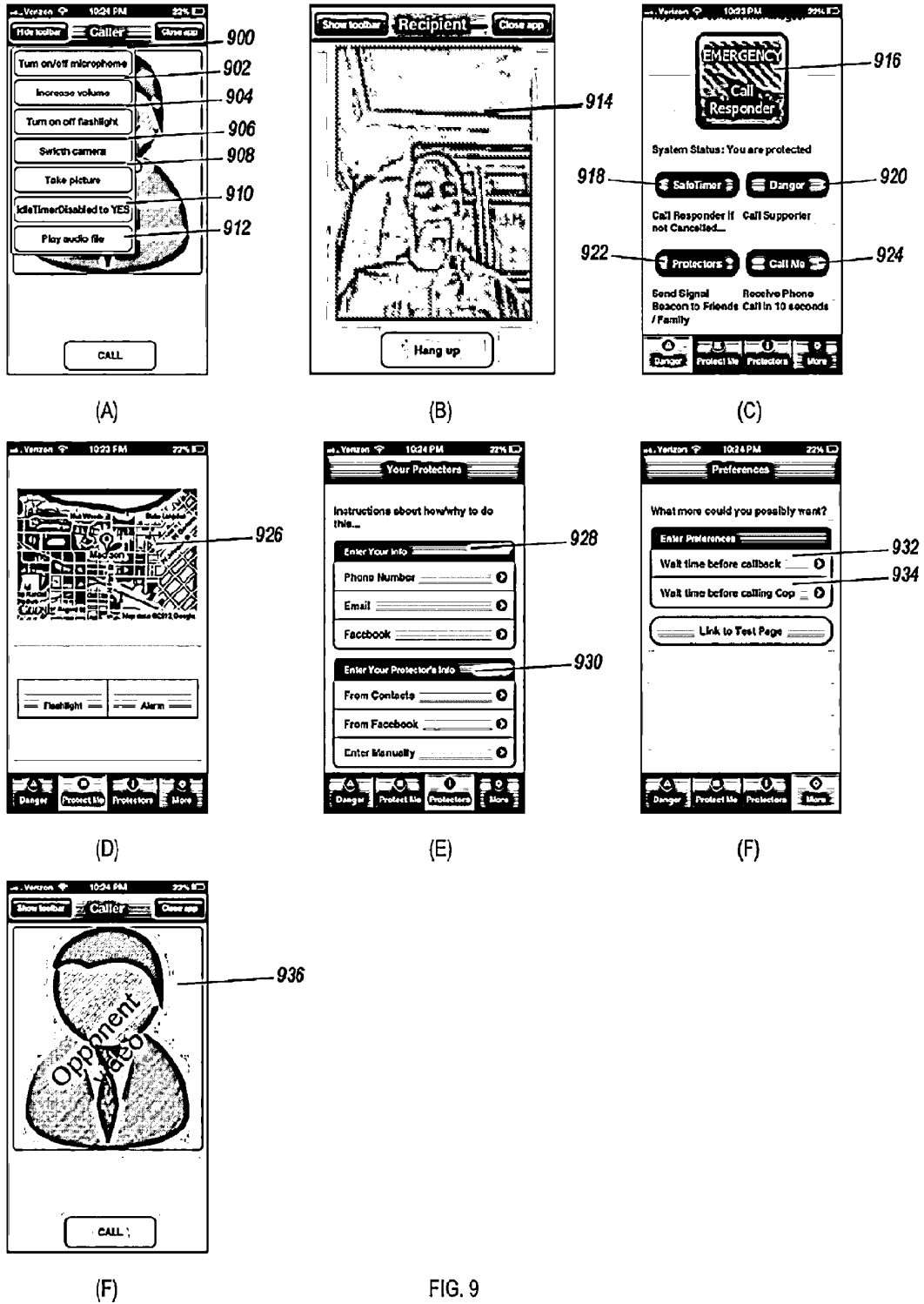


FIG. 9

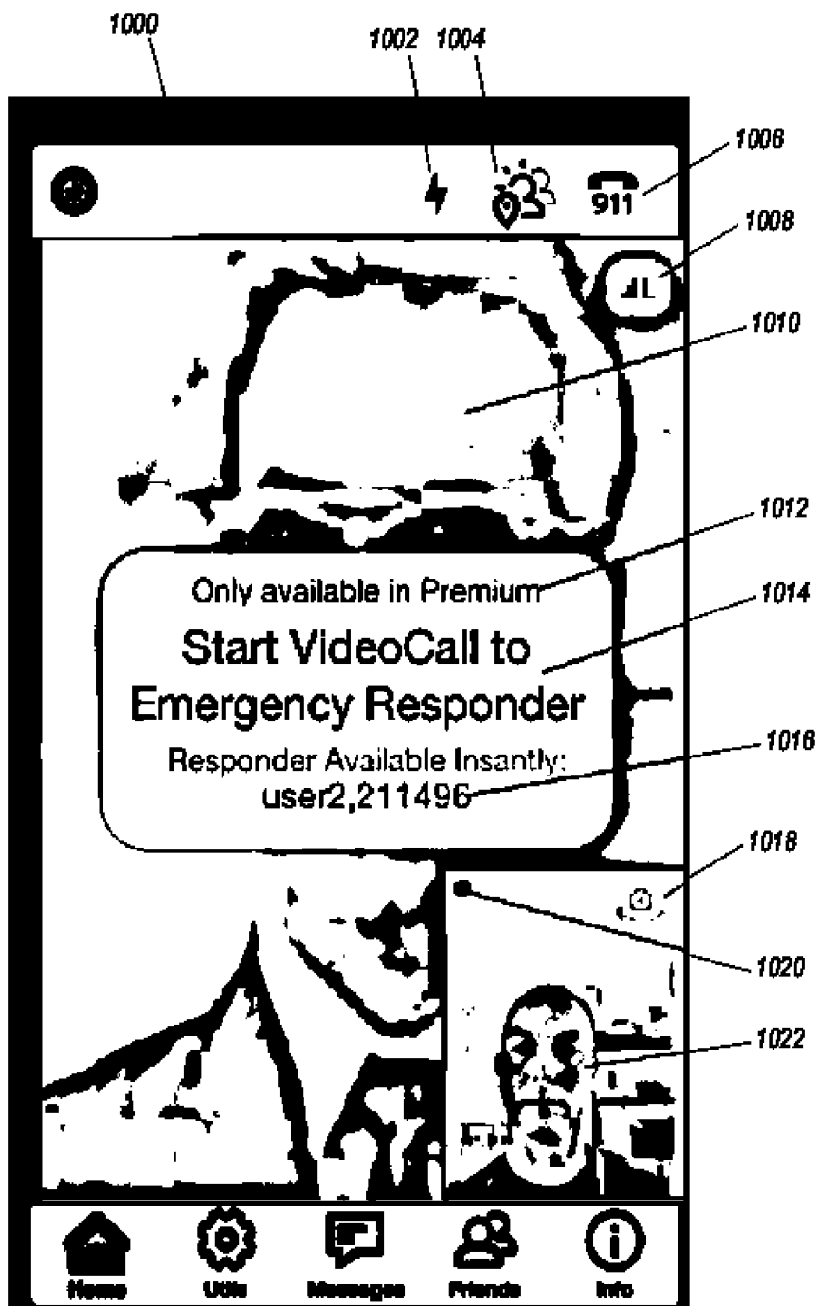


FIG. 10

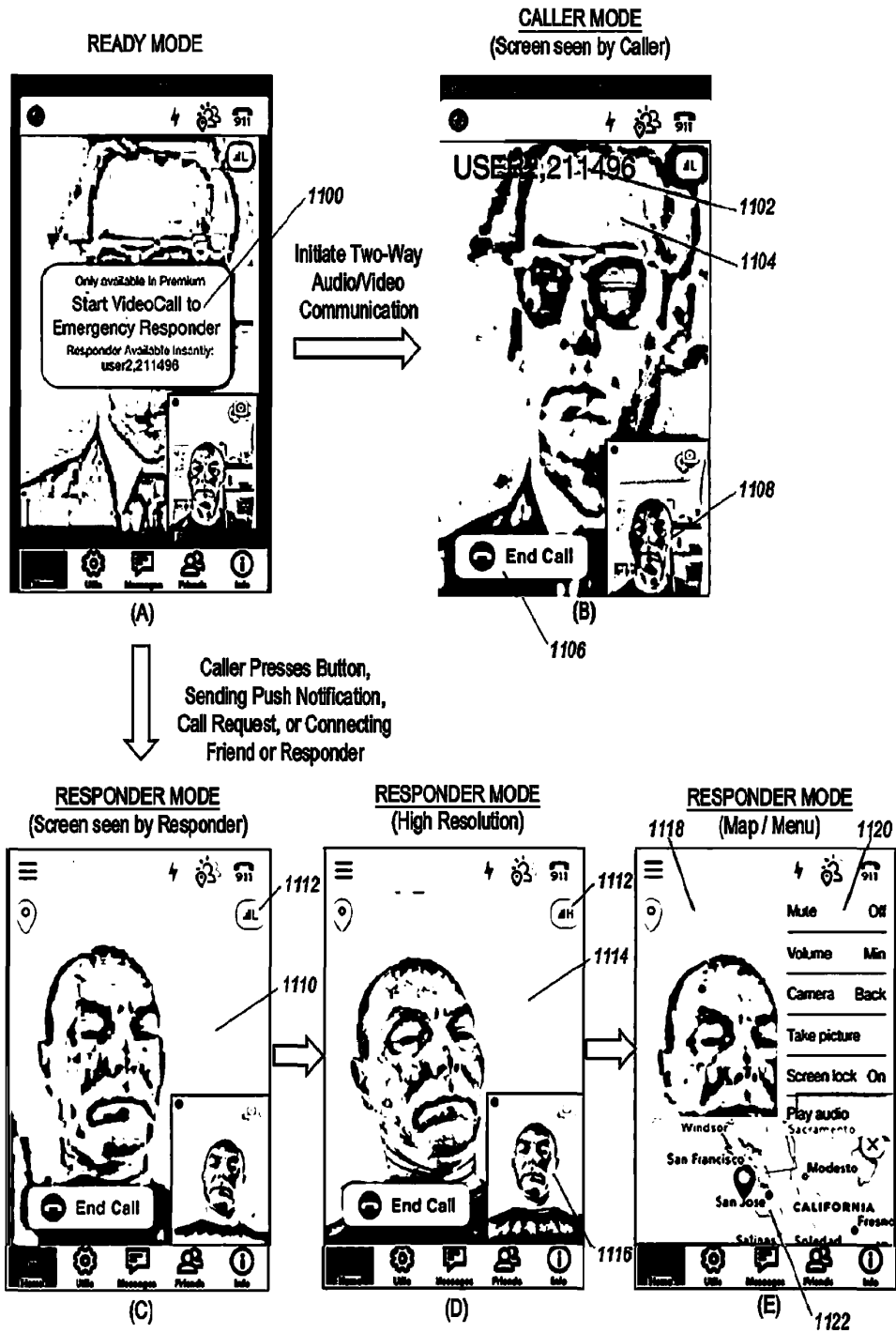


FIG. 11

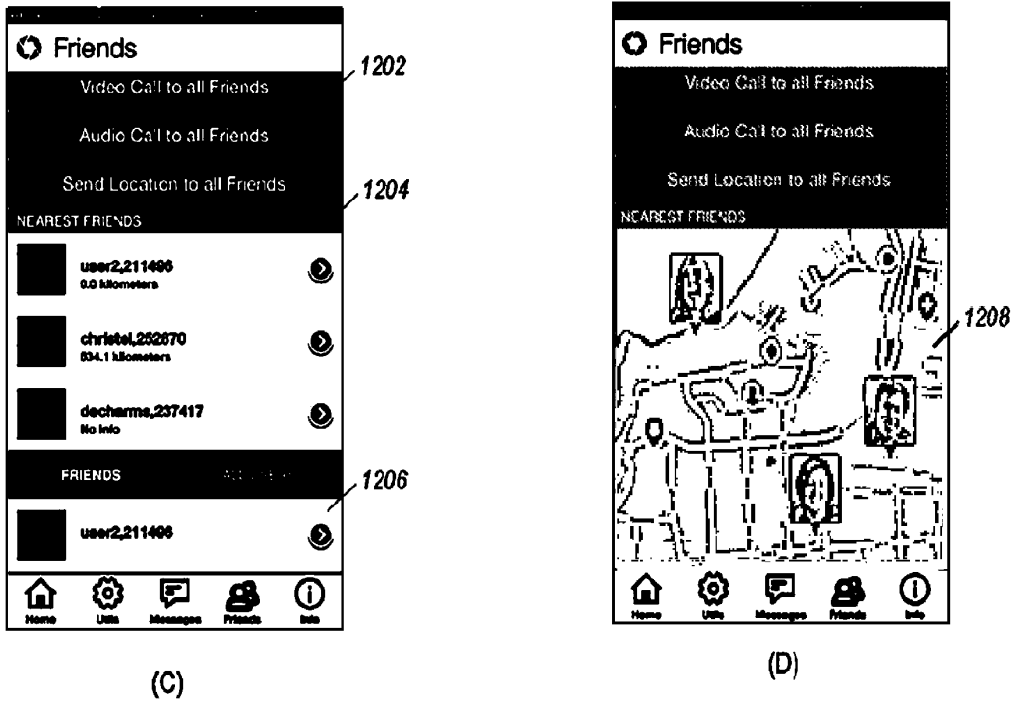
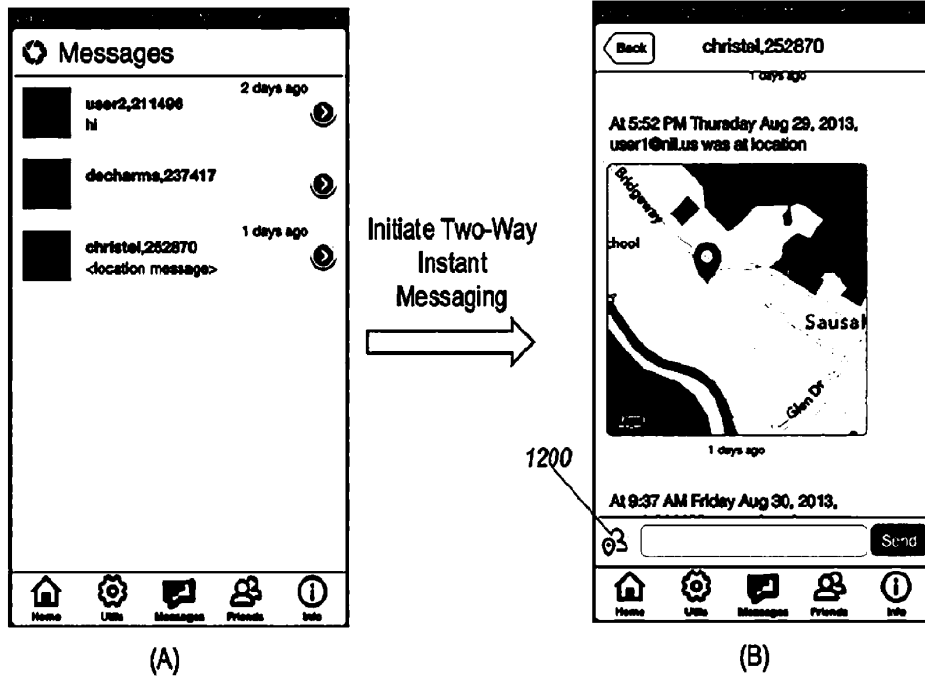


FIG. 12

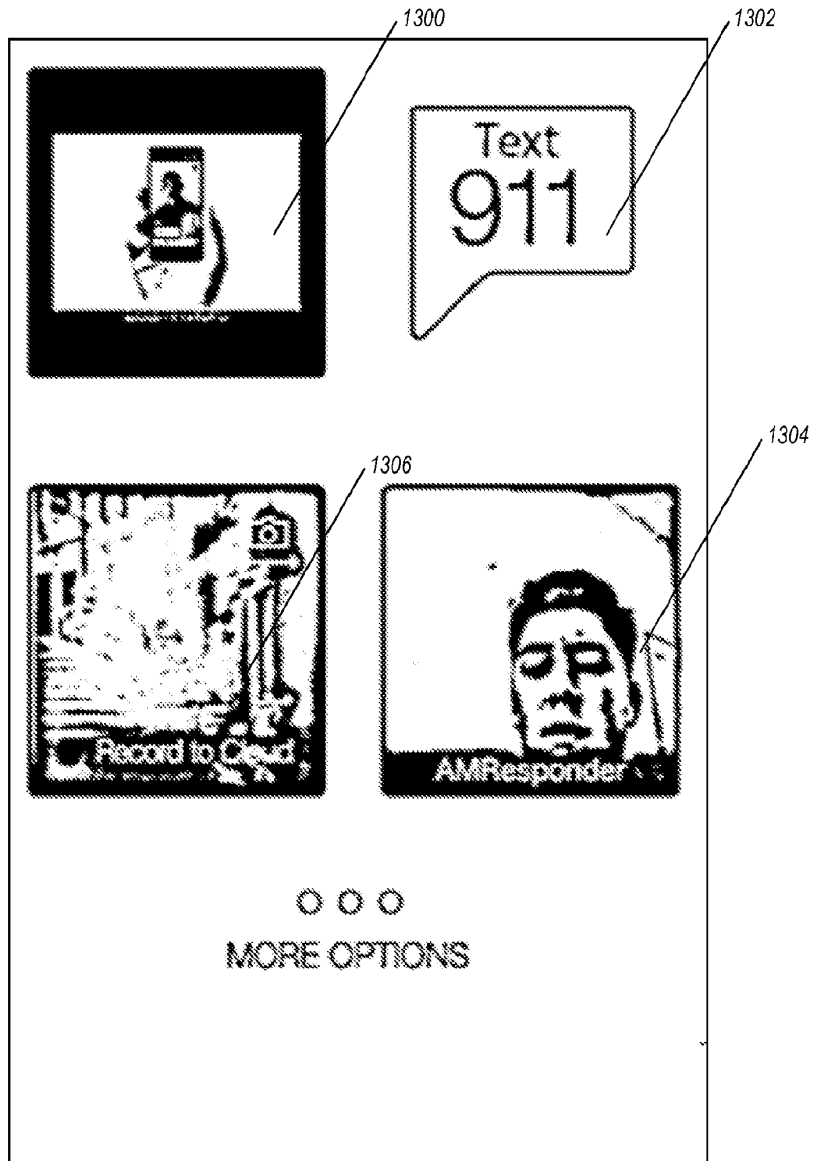


FIG. 13

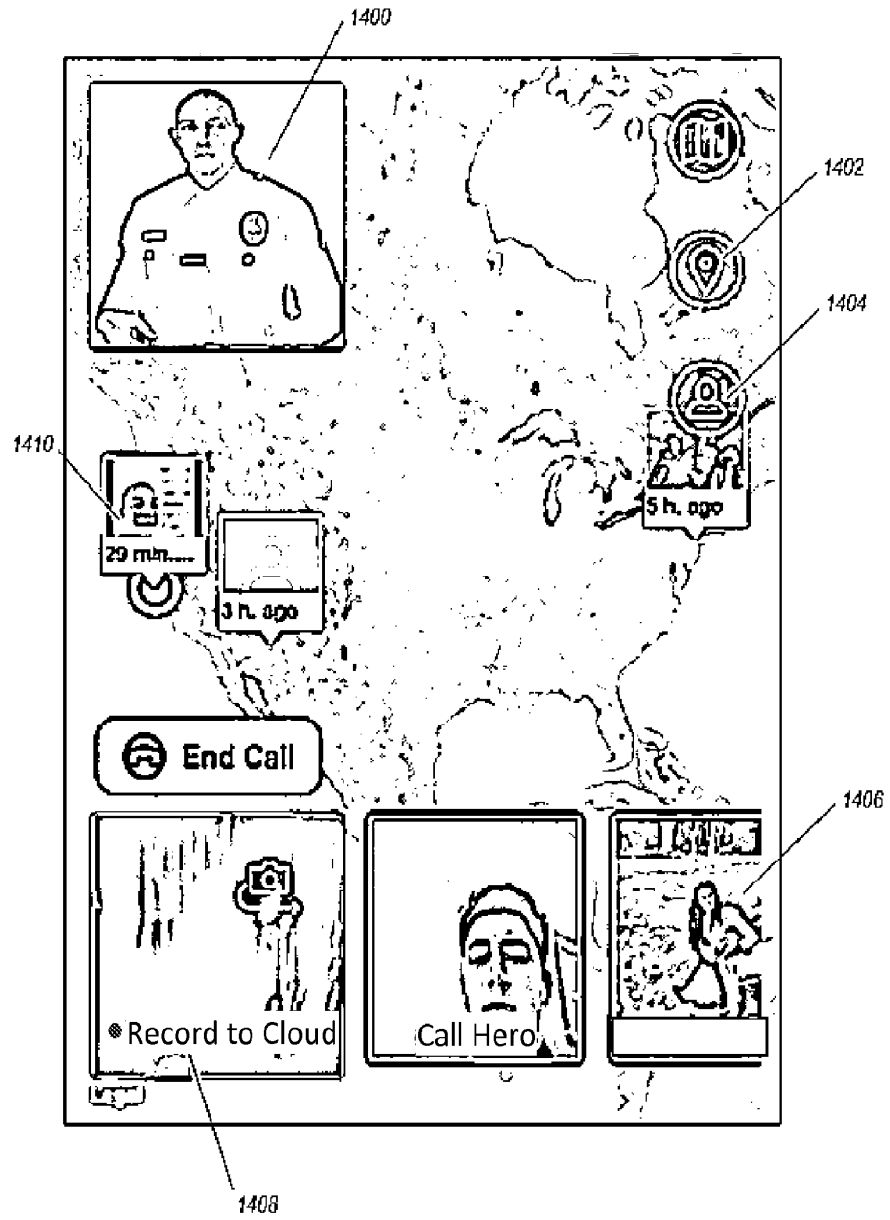


FIG. 14

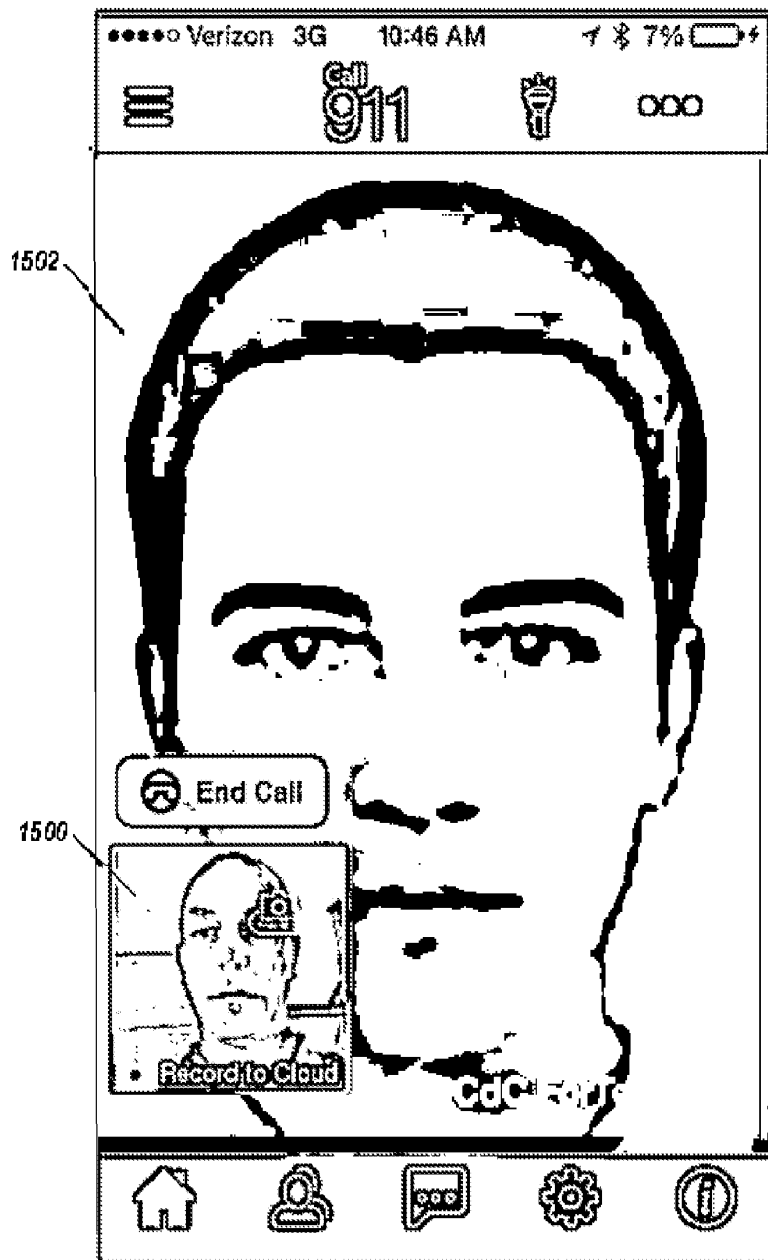


FIG. 15

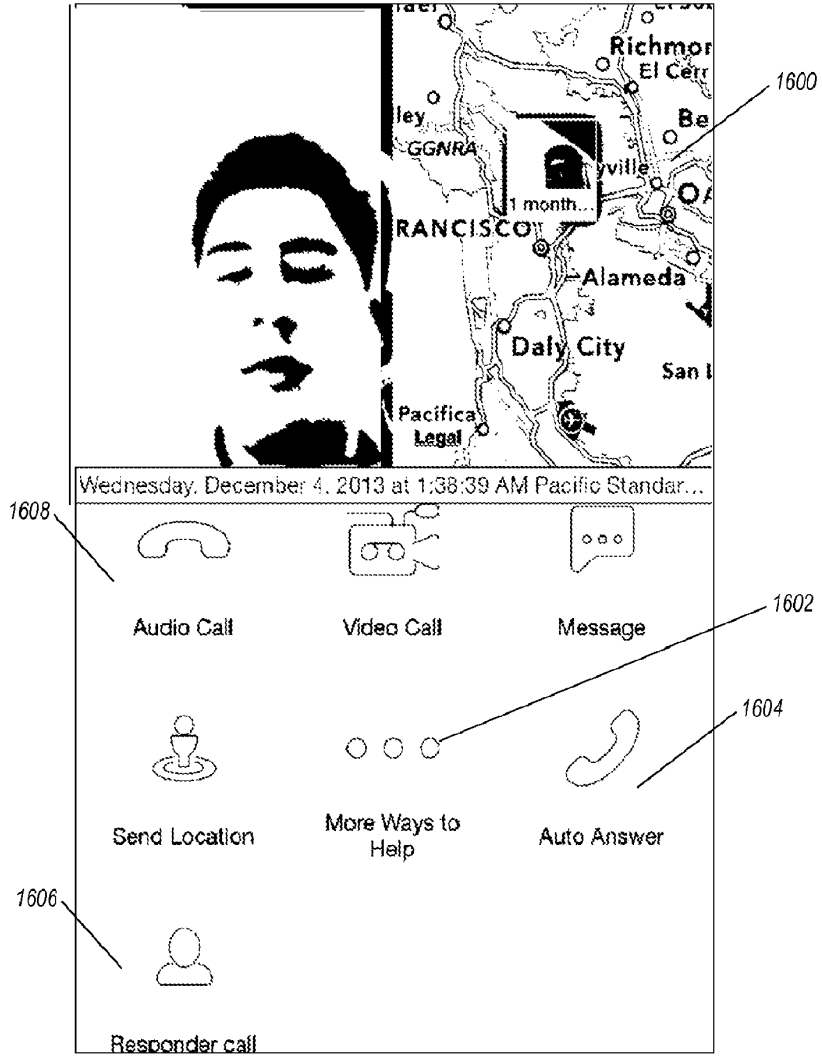


FIG. 16

Settings

Picture:	NO PHOTOS	
Age:	48	⌵
Height:	6 feet 2 inches	⌵
Weight:	Select weight...	⌵
Hair color:	Select hair color...	⌵
Eye color:	Select...	⌵
Other Name(s):	Add your other name(s) here.	
First Language:	Select...	⌵
Second Language:	Select...	⌵
Country:	Select...	⌵
<ul style="list-style-type: none"> • Home address (tap to edit) • Work address (tap to edit) • Billing address (tap to edit) 		
Safe word:	Add one word here. This will be your safe word.	
<hr/>		
Health		
Allergies:	Add your allergies here.	⌵
Health conditions (if any):	Add your health conditions here (if any).	⌵
Health information:	Add your health information here (if available).	⌵
<hr/>		
Automobile		
Ignore this section if you don't have a car.		
Auto make:	Select an auto make...	⌵
Auto model:	Add the model of your auto here.	
Auto year:	Select year...	⌵
Auto color:	Select a color...	⌵
<hr/>		
Security Questions		
These are used to prove your identity if you lose access to your account.		
Security question 1:	Select a question...	⌵
Answer 1:		

FIG. 18A

Security Questions

These are used to prove your identity if you lose access to your account.

Security question 1: Select a question...

Answer 1:

Security question 2: Select a question...

Answer 2:

Security question 3: Select a question...

Answer 3:

Emergency contacts

- o Emergency contact 1 (tap to edit)
- * Emergency contact 2 (tap to edit)

Save

FIG. 18B

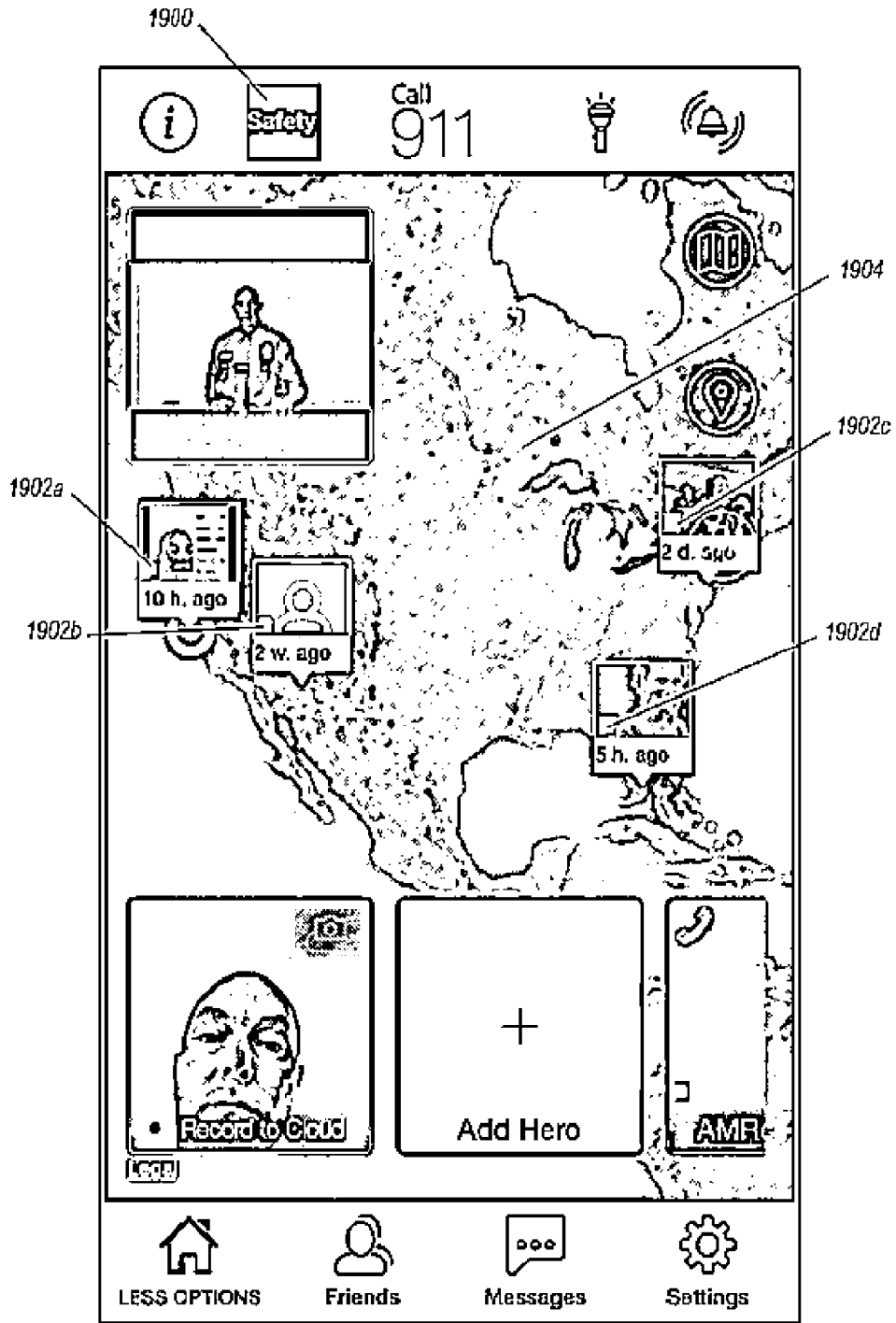


FIG. 19

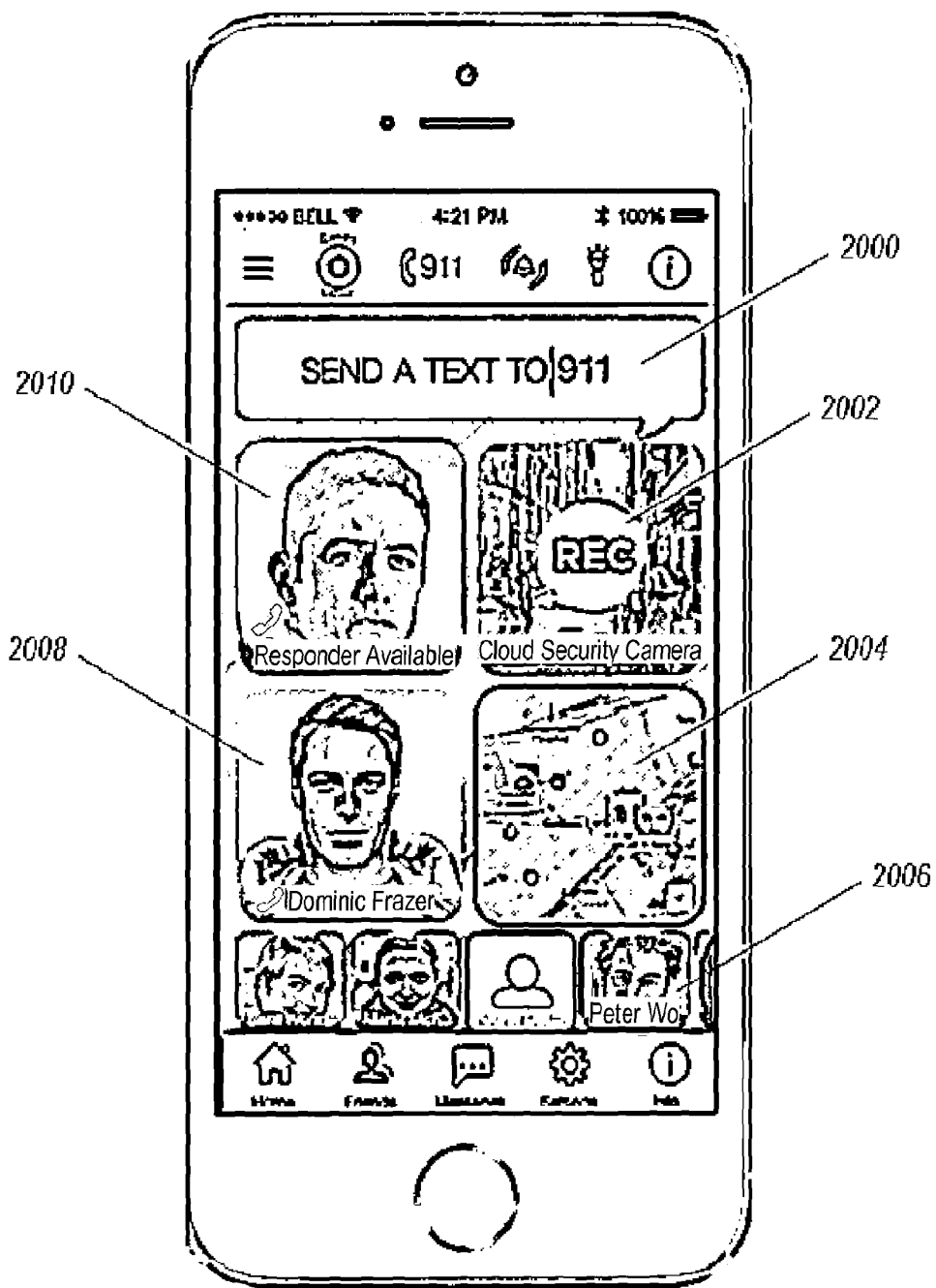


FIG. 20

Text
911

This is a testing message. Please ignore.

By clicking the "Send text to emergency responders..." button, you accept that the information you are submitting is true to the best of your knowledge.

Send text to 911 emergency responders

Optional details

Type of incident:
Select type of incident...

(Optional) Picture or Video to include:
Choose File No file chosen

Dispatch Police/Emergency Services to this location.

Police/Emergency Services can call me on this phone number for more information.

When you tap on the "send report" button, your information, incident type and comment will be sent to the incident team. Your user information will be sent too, but will not be visible to other users.

2100

2102

2104

2106

2108

2110

FIG. 21

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 61819575 A [0001]
- US 61872690 A [0001]
- US 61924901 A [0001]
- US 20110111728 A1 [0004]
- US 20130040600 A1 [0005]

Non-patent literature cited in the description

- **LAYNE HOLLEY ; MICHAEL BLAIR.** Call Center Management on Fast Forward: Succeeding in the New Era of Customer Relationships. 08 May 2012 [0246]



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/943,956	09/13/2022	Alexander Dizengof	3010043.2	2316
46019	7590	11/25/2022	EXAMINER	
BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX) TWO NORTH CENTRAL AVENUE, SUITE 2100 PHOENIX, AZ 85004			LAFONTANT, GARY	
			ART UNIT	PAPER NUMBER
			2646	
			NOTIFICATION DATE	DELIVERY MODE
			11/25/2022	ELECTRONIC

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

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

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

PXBCIPDocketing@bcplaw.com

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Claim Rejections - 35 USC § 103

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

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains.

Patentability shall not be negated by the manner in which the invention was made.

Claim(s) 1-20 are rejected under **35 U.S.C. 103** as being unpatentable over **Piett (US 2016/0337831 A1)** in view of **Somers (US 2015/0106528 A1)**.

Regarding Claims 1, 8, 15

Piett discloses a method implemented via execution of computing instructions **(See {0016}; [0040]; instructions to perform method)** configured to run at one or more processors **(Fig.1(108)(Fig.1(110)))**,

the method comprising:

obtaining a phone number **(See [0043]; [0060-0062]; obtaining at least one of the unique identifier including MSID)** of a mobile device **(Fig.1(102))** used by a user **(See [0043]; a user initiating communication)** making an emergency call **(See [0043]; during emergency call);**

wherein the emergency call is conducted with a recipient **(Fig.1(108))** through a first connection **(See [0043]; emergency through cellular communications to PSAP recipient);**

transmitting a uniform resource locator (URL) to the mobile device **(Fig.1(102))** through an electronic message **(See [0022]; [0062-0065]; mobile device received URI message to initiate transmission of data through network 106, URI comprises URL),**

wherein the electronic message **(See [0022]; initiation message is transmitted to calling device to start transmission)** is transmitted through a second connection **(See Fig.1(106); [0022]; [0039]; [0042-0043]; OTSL communicate with calling device via network 106)** using the phone number

(See [0043]; [0060-0062]; obtaining at least one of the unique identifier including Message ID),

wherein the second connection is different from the first connection **(See Fig.1; cellular network 104 different than packet network 106),**

But **Piett** fails to explicitly recite

wherein the electronic message allows the user to click on the URL to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit real-time video stream from the mobile device, and

wherein the URL is associated with the phone number of the mobile device

receiving the real-time video stream from the mobile device through the WebRTC session; and

sending the real-time video stream to the recipient for display on a screen of the recipient,

wherein the real-time video stream is associated with a unique identifier for the mobile device.

However in analogous art,

Somers teaches about creating a streaming video session between two communication devices in a network using WebRTC session protocol providing hyperlink to the streaming device **(See [0007]; [0013]; [0047]; [0062]; hyperlink is provided to user to start streaming data);**

wherein the URL is associated with the phone number of the mobile device **(See [0016]; [0047]; caller info associated with URI);**

receiving the real-time video stream from the mobile device through the WebRTC session **(See [0007]; [0013]; [0017]; [0060]; real time video data streaming);**
and

sending the real-time video stream to the recipient for display on a screen of the recipient **(See [0020]; [0084]; end user display of video),**

wherein the real-time video stream is associated with a unique identifier for the mobile device **(See [0016-0017]; [0047]; WebRTC associated with identifier of UE) .**

Piett and Somers are analogous art because they all pertain to streaming data using network communication channel between two communication devices using different communication protocol. **Piett** teaches about setting up an emergency call through a calling device to a PSAP. The latter then requesting a location data of the calling device. **Somers** teaches about setting up WebRTC between users though web link using device identities to stream audio and video data. **Piett** could use **Somers** features to stream video data of caller surrounding experiencing emergency situation. Therefore it would have been obvious at the time of the filing of the application for one of ordinary skill to combine **Piett** and **Somers** as to obtain an efficient emergency rescue communication system.

Regarding Claim 2, 9, 16

Piett and Somers teach all the features with respect to **claim 1, 8, 15 and Piett** further teaches

wherein the recipient is at least one of
an emergency call center (**Fig,1(108); PSAP/dispatch**)
or
a dispatch unit (**See [0013]; [0040]; PSAP/dispatch**).

Regarding Claim 3, 10, 17

Piatt and Somers teach all the features with respect to **claim 1, 8, 15 and Piatt** further teaches

wherein at least one of:

the first connection is a voice call over a cellular network (**See [0036-0037]; emergency call**);

the electronic message is a text message (**See [0038]; emergency text**); or

the second connection is a text messaging service (**See [0086]; text message to caller**).

Regarding Claim 4, 11, 18

Piatt and Somers teach all the features with respect to **claim 1, 8, 15 and Piatt** further teaches

wherein the unique identifier comprises the phone number of the mobile device (**See [0043]; [0047]; [0060-0062]; phone number retrieved from transmission message**) .

Regarding Claim 5, 12, 19

Piett and Somers teach all the features with respect to **claim 1, 8, 15 and Somers**

further teaches

wherein the real-time video stream (**See [0007]; [0013]**) is transmitted from the mobile device (**Fig.1(120)**) to the recipient (**Fig.1(115)**) through a server (**Fig.1(110)**) that is separate from the mobile device and the recipient (**See Fig.1; Fig.2(A-D); [0043]**).

Regarding Claim 6, 13, 20

Piett and Somers teach all the features with respect to **claim 5, 12, 15 and Somers**

further teaches

wherein the server is a proxy server (**See {0036-0037}**) configured to convert a data format of the real-time video stream (**See [0042-0044]; [0048-0049]; select format on how to present data through the network**).

Regarding Claim 7, 14

Piett and Somers teach all the features with respect to **claim 1, 8 and Piett** further

teaches

wherein the session further transmits at least one of

(i) GPS location data of the mobile device for display on the screen of the recipient (**See [0025]; [0043]; [0060]; location data is provided to be displayed**) or

(ii) one or more photographs taken on the mobile device for display on the screen of the recipient.

(The term “ at least one” translate to the satisfaction of one or more of the limitation can be analyzed)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to GARY LAFONTANT whose telephone number is (571)272-3037. The examiner can normally be reached 9:00AM -5:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lester Kincaid can be reached on 571-272-7922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: <https://patentcenter.uspto.gov>. Visit <https://www.uspto.gov/patents/apply/patent->

center for more information about Patent Center and

<https://www.uspto.gov/patents/docx> for information about filing in DOCX format. For

additional questions, contact the Electronic Business Center (EBC) at 866-217-9197

(toll-free). If you would like assistance from a USPTO Customer Service

Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

**/GARY LAFONTANT/
Examiner, Art Unit 2646**

Notice of References Cited	Application/Control No. 17/943,956	Applicant(s)/Patent Under Reexamination Dizengof, Alexander	
	Examiner GARY LAFONTANT	Art Unit 2646	Page 1 of 1

U.S. PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A US-20150106528-A1	04-2015	Somes; Brian	H04L65/00	709/228
*	B US-20160337831-A1	11-2016	Piett; William Todd	H04M3/42357	1/1
C					
D					
E					
F					
G					
H					
I					
J					
K					
L					
M					


FOREIGN PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
N					
O					
P					
Q					
R					
S					
T					

NON-PATENT DOCUMENTS

*	U	V	W	X
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)			

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<i>Search Notes</i> 	Application/Control No. 17/943,956	Applicant(s)/Patent Under Reexamination Dizengof, Alexander
	Examiner GARY LAFONTANT	Art Unit 2646

CPC - Searched*		
Symbol	Date	Examiner
All	11/18/2022	GL

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Pe2E Search	11/18/2022	GL

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner

/GARY LAFONTANT/ Examiner, Art Unit 2646	
---	--

PE2E SEARCH - Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	British Equivalents	Time Stamp
L1	8	"20150106528"	(US-PGPUB; USPAT; USOCR; FIT (AU, AP, AT, CA, CH, CN, DD, DE, EA, EP, ES, FR, GB, JP, KR, OA, RU, SU, WO); FPRS; EPO; JPO; DERWENT; IBM_TDB)	OR	ON	ON	2022/11/18 04:21 PM
L2	2	"20150106528"	(US-PGPUB; USPAT)	OR	ON	ON	2022/11/18 04:21 PM
L3	2	"20160337831"	(US-PGPUB; USPAT)	OR	ON	ON	2022/11/18 04:22 PM

PE2E SEARCH - Search History (Interference)

There are no Interference searches to show.

Bibliographic Data

Application No: 17/943,956

Foreign Priority claimed: Yes No

35 USC 119 (a-d) conditions met: Yes No Met After Allowance

Verified and Acknowledged:

Examiner's Signature

Initials

Title:

SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM
FOR STREAMING REAL-TIME DATA FROM A USER DEVICE

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/13/2022	455	2646	3010043.2
RULE			

APPLICANTS

Carbyne Ltd.,

INVENTORS

Alexander Dizengof, Ashdod, ISRAEL

CONTINUING DATA

This application is a CON of 17492757 10/04/2021

17492757 is a CON of 16901074 06/15/2020 PAT 11139996

16901074 is a CON of 15822927 11/27/2017 PAT 10686618

15822927 has PRO of 62544835 08/13/2017

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

09/28/2022

** SMALL ENTITY **

STATE OR COUNTRY

ISRAEL

ADDRESS

BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX)

TWO NORTH CENTRAL AVENUE, SUITE 2100

PHOENIX, AZ 85004

UNITED STATES

FILING FEE RECEIVED

\$3,000



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/943,956	09/13/2022	Alexander Dizengof	3010043.2	2316
46019	7590	10/28/2022	EXAMINER	
BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX) TWO NORTH CENTRAL AVENUE, SUITE 2100 PHOENIX, AZ 85004			CENTRAL, DOCKET	
			ART UNIT	PAPER NUMBER
			OPAP	
			NOTIFICATION DATE	DELIVERY MODE
			10/28/2022	ELECTRONIC

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

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

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

PXBCIPDocketing@bcplaw.com

<i>Decision Granting Request for Prioritized Examination (Track I)</i>	Application No. 17/943,956	Applicant(s) Dizengof, Alexander	
	Examiner FIKIRTE A GEREMEW	Art Unit OMBL	AIA (FITF) Status Yes
<p>1. THE REQUEST FILED <u>13 September 2022</u> IS GRANTED .</p> <p>The above-identified application has met the requirements for prioritized examination</p> <p>A. <input checked="" type="checkbox"/> for an original nonprovisional application (Track I).</p> <p>B. <input type="checkbox"/> for an application undergoing continued examination (RCE).</p> <p>2. The above-identified application will undergo prioritized examination. The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:</p> <p>A. filing a <u>petition for extension of time</u> to extend the time period for filing a reply;</p> <p>B. filing an <u>amendment to amend the application to contain more than four independent claims, more than thirty total claims</u>, or a multiple dependent claim;</p> <p>C. filing a <u>request for continued examination</u> ;</p> <p>D. filing a notice of appeal;</p> <p>E. filing a request for suspension of action;</p> <p>F. mailing of a notice of allowance;</p> <p>G. mailing of a final Office action;</p> <p>H. completion of examination as defined in 37 CFR 41.102; or</p> <p>I. abandonment of the application.</p> <p>Telephone inquiries with regard to this decision should be directed to FIKIRTE GEREMEW at (703) 756-1930. In his/her absence, calls may be directed to Petition Help Desk at (571) 272-3282.</p>			
/FIKIRTE A GEREMEW/ PROGRAM SUPPORT ASSISTANT, OMBL			



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, TOT CLAIMS, IND CLAIMS. Row 1: 17/943,956, 09/13/2022, OPAP, 3000, 3010043.1, 20, 3

CONFIRMATION NO. 2316

CORRECTED FILING RECEIPT



46019
BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX)
TWO NORTH CENTRAL AVENUE, SUITE 2100
PHOENIX, AZ 85004

Date Mailed: 10/18/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Alexander Dizengof, Ashdod, ISRAEL;

Applicant(s)

Carbyne Ltd., Tel-Aviv, ISRAEL;

Assignment For Published Patent Application

Carbyne Ltd., Tel-Aviv, ISRAEL

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 17/492,757 10/04/2021
which is a CON of 16/901,074 06/15/2020 PAT 11,139,996
which is a CON of 15/822,927 11/27/2017 PAT 10,686,618
which claims benefit of 62/544,835 08/13/2017

Foreign Applications for which priority is claimed (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 09/28/2022

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 17/943,956**

Projected Publication Date: 01/05/2023

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE

Preliminary Class

455

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

page 2 of 4

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 4 columns: APPLICATION NUMBER (17/943,956), FILING OR 371(C) DATE (09/13/2022), FIRST NAMED APPLICANT (Alexander Dizengof), ATTY. DOCKET NO./TITLE (3010043.1)

CONFIRMATION NO. 2316

NEW OR REVISED PPD NOTICE

46019
BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX)
TWO NORTH CENTRAL AVENUE, SUITE 2100
PHOENIX, AZ 85004



NOTICE OF NEW OR REVISED PROJECTED PUBLICATION DATE

The above-identified application has a new or revised projected publication date. The current projected publication date for this application is 01/05/2023. If this is a new projected publication date (there was no previous projected publication date), the application has been cleared by Licensing & Review or a secrecy order has been rescinded and the application is now in the publication queue.

If this is a revised projected publication date (one that is different from a previously communicated projected publication date), the publication date has been revised due to processing delays in the USPTO or the abandonment and subsequent revival of an application. The application is anticipated to be published on a date that is more than six weeks different from the originally-projected publication date.

More detailed publication information is available through the private side of Patent Application Information Retrieval (PAIR) System. The direct link to access PAIR is currently http://pair.uspto.gov. Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Questions relating to this Notice should be directed to the Office of Data Management, Application Assistance Unit at (571) 272-4000, or (571) 272-4200, or 1-888-786-0101.



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, TOT CLAIMS, IND CLAIMS. Row 1: 17/943,956, 09/13/2022, 830, 3010043.1, 20, 3

CONFIRMATION NO. 2316

FILING RECEIPT



46019
BRYAN CAVE LEIGHTON PAISNER LLP (PHOENIX)
TWO NORTH CENTRAL AVENUE, SUITE 2100
PHOENIX, AZ 85004

Date Mailed: 09/30/2022

Receipt is acknowledged of this non-provisional utility patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF FIRST INVENTOR, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection.

Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a corrected Filing Receipt, including a properly marked-up ADS showing the changes with strike-through for deletions and underlining for additions. If you received a "Notice to File Missing Parts" or other Notice requiring a response for this application, please submit any request for correction to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections provided that the request is grantable.

Inventor(s)

Alexander Dizengof, Ashdod, ISRAEL;

Applicant(s)

Carbyne Ltd., Tel-Aviv, ISRAEL;

Assignment For Published Patent Application

Carbyne Ltd., Tel-Aviv, ISRAEL

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 17/492,757 10/04/2021
which is a CON of 16/901,074 06/15/2020 PAT 11,139,996
which is a CON of 15/822,927 11/27/2017 PAT 10,686,618
which claims benefit of 62/544,835 08/13/2017

Foreign Applications for which priority is claimed (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

Projected Publication Date: 01/05/2023

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number
17/943,956

APPLICATION AS FILED - PART I

		(Column 1)	(Column 2)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
FOR		NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)
BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A	N/A	80		N/A	
SEARCH FEE (37 CFR 1.16(k), (l), or (m))		N/A	N/A	N/A	350		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A	N/A	400		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))		20 minus 20 =	*	0	x =	0		
INDEPENDENT CLAIMS (37 CFR 1.16(h))		3 minus 3 =	*	0	x =	0		
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).							
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))								
				TOTAL	830		TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED - PART II

		(Column 1)	(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		x =	
	Application Size Fee (37 CFR 1.16(s))								
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
				TOTAL ADD'L FEE			TOTAL ADD'L FEE		
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		x =	
	Application Size Fee (37 CFR 1.16(s))								
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
				TOTAL ADD'L FEE			TOTAL ADD'L FEE		

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.



**CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION
 UNDER 37 CFR 1.102(e)** (Page 1 of 1)

First Named Inventor:	Alexander Dizengof	Nonprovisional Application Number (if known):	
Title of Invention:	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently \$0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.
2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.
3. The applicable box is checked below:
 - I. **Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)**
 - i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.
 ---OR---
 - (b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.
 - ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, or the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.
 - II. **Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)**
 - i. A request for continued examination has been filed with, or prior to, this form.
 - ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
 - iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
 - iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
 - v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature	/Cory Smith/	Date	September 13, 2022
Name (Print/Typed)	Cory Smith	Practitioner Registration Number	63,218

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

*Total of 1 forms are submitted.

Privacy Act Statement

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

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

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

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.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3010043.1
		Application Number	
Title of Invention	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2:

Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor	1				Remove
Legal Name					
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Alexander		Dizengof		
Residence Information (Select One) US Residency • Non US Residency Active US Military Service					
City	Ashdod	Country of Residence ⁱ	L		
Mailing Address of Inventor:					
Address 1	11B Eliyahu HaNavi Street				
Address 2					
City	Ashdod	State/Province			
Postal Code	7747044	Country ⁱ	IL		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
<input type="checkbox"/> An Address is being provided for the correspondence information of this application.			
Customer Number	46019		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE		
Attorney Docket Number	3010043.1	Small Entity Status Claimed	<input checked="" type="checkbox"/>
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	3	Suggested Figure for Publication (if any)	

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.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3010043.1
		Application Number	
Title of Invention	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE		

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

Request Early Publication (Fee required at time of Request 37 CFR 1.219)

Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer number will be used for the Representative Information during processing.

Please Select One:	<input checked="" type="radio"/> Customer Number	<input type="radio"/> US Patent Practitioner	<input type="radio"/> Limited Recognition (37 CFR 11.9)
Customer Number	46019		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.

When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status	Pending	<input type="button" value="Remove"/>	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	17/492757	2021-10-04

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.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3010043.1			
		Application Number				
Title of Invention	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE					
Prior Application Status	Patented				Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)	
17/492757	Continuation of	16/901074	2020-06-15	11139996	2021-10-05	
Prior Application Status	Patented				Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)	
16/901074	Continuation of	15/822927	2017-11-27	10686618	2020-06-16	
Prior Application Status	Expired				Remove	
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)			
15/822927	Claims benefit of provisional	62/544835	2017-08-13			
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.						Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)ⁱ the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

			Remove
Application Number	Country ⁱ	Filing Date (YYYY-MM-DD)	Access Code ⁱ (if applicable)
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

- This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
- NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3010043.1
		Application Number	
Title of Invention	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE		

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

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.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3010043.1
		Application Number	
Title of Invention	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE		

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.			
Applicant	1	<input type="button" value="Remove"/>	
If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.			
<input type="button" value="Clear"/>			
<input checked="" type="radio"/> Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor	
Person to whom the inventor is obligated to assign.		Person who shows sufficient proprietary interest	
If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:			
<input type="button" value="Clear"/>			
Name of the Deceased or Legally Incapacitated Inventor: <input type="text"/>			
If the Applicant is an Organization check here. <input checked="" type="checkbox"/>			
Organization Name	Carbyne Ltd.		
Mailing Address Information For Applicant:			
Address 1	94 Yigal Alon Street (South Building)		
Address 2			
City	Tel-Aviv	State/Province	
Country	IL	Postal Code	6789139
Phone Number		Fax Number	
Email Address			
Additional Applicant Data may be generated within this form by selecting the Add button. <input type="button" value="Add"/>			

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	3010043.1
	Application Number	
Title of Invention	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE	

Assignee	1		
Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.			
			<input type="button" value="Remove"/>
If the Assignee or Non-Applicant Assignee is an Organization check here. <input checked="" type="checkbox"/>			
Organization Name	Carbyne Ltd.		
Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1	94 Yigal Alon Street (South Building)		
Address 2			
City	Tel-Aviv	State/Province	
Country i	L	Postal Code	6789139
Phone Number		Fax Number	
Email Address			
Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Cory Smith/		Date (YYYY-MM-DD)	2022-09-13	
First Name	Cory	Last Name	Smith	Registration Number	63218
Additional Signature may be generated within this form by selecting the Add button.				<input type="button" value="Add"/>	

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.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	3010043.1
		Application Number	
Title of Invention	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE		

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

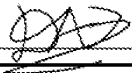
The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection 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.

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

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE
<p>As the below named inventor, I hereby declare that:</p> <p>This declaration is directed to: <input checked="" type="checkbox"/> The attached application, or <input type="checkbox"/> United States application or PCT international application number _____ filed on _____.</p> <p>The above-identified application was made or authorized to be made by me.</p> <p>I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.</p> <p>I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.</p> <p style="text-align: center;">WARNING:</p> <p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.</p>	
<p>LEGAL NAME OF INVENTOR</p> <p>Inventor: <u>Alexander Dizengof</u> Date (Optional): <u>09/13/2022</u></p> <p>Signature: <u></u></p>	
<p>Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.</p>	

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1 minute 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. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, 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 disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES UTILITY PATENT APPLICATION

Title: **SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR
STREAMING REAL-TIME DATA FROM A USER DEVICE**

Inventor: **Alexander Dizengof
Ashdod, Israel**

Assignee: **Carbyne Ltd.
Tel-Aviv, Israel**

Attorneys: Bryan Cave Leighton Paisner LLP
Two North Central Avenue, Suite 2100
Phoenix, Arizona 85004-4406
Telephone: (602) 364-7000

**SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING
REAL-TIME DATA FROM A USER DEVICE**

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. Patent Application No. 17/492,757, filed on October 4, 2021, which is a continuation of U.S. Patent Application No. 16/901,074, filed on June 15, 2020, now U.S. Patent No. 11,139,996, which is a continuation of U.S. Patent Application No. 15/822,927, filed on November 27, 2017, now U.S. Patent No. 10,686,618, which claims the benefit of U.S. Provisional Application No. 62/544,835, filed on August 13, 2017. U.S. Provisional Application No. 62/544,835 and U.S. Patent Application Nos. 17/492,757, 16/901,074, and 15/822,927 are incorporated herein by reference in their entirety.

FIELD AND BACKGROUND OF THE INVENTION

[0002] The present disclosure relates generally to streaming of data, and more specifically, to a method and system of streaming data from a user device without the need to download and install a specialized application.

[0003] Many mobile devices on the market today, including smartphones, tablets, notebook computers, and the like, come equipped with built-in media capturing components, including still cameras, video cameras, microphones, global positioning receivers, and the like. These components are used by millions of users to share photos and videos, use the internet for video chats, navigate roads with ease, along with a multitude of other uses.

[0004] However, when a person calls an emergency or municipal dispatch unit to report an incident from a mobile device, these media capturing capabilities are rarely used. Rather, an operator of a call center, such as a public-safety answering point (PSAP), receives the incoming calls, asks the caller several questions to assess the nature of the incident, and then delivers the call to a suitable dispatch unit, such as police, firefighting, ambulance services, and the like.

- [0005] In many cases the calls received at these call centers are critical and every additional detail that can be retrieved from the call may help the dispatch operator better understand the situation in the field, and explain to the dispatched forces the situation before they arrive on-scene so they can be better prepared.
- [0006] Some communication applications allow the device to connected to a dispatch unit system, by which audio, video, messages, and the like can be transmitted to the call center system. Thus, the dispatch operator is able to hear the user, see video captured in real time by the user's device, e.g., a smart phone or tablet, send and receive text messages, identify the communication device location, and the like.
- [0007] However, these proposed systems require a user to download and install specialized applications, which may take time, losing precious moments of data. Further, in many emergency situations involving large numbers of individuals, available bandwidth of cellular networks become limited, as many devices attempt to connect the cellular networks at the same time. As such, communication and access to download applications over a cellular network may become unfeasible. Additionally, individuals experiencing a stressful emergency situation may be unfocused and unable to operate a previously installed application, let alone download and set up a new application on their devices.
- [0008] It would therefore be advantageous to provide a solution that would overcome the challenges noted above.

SUMMARY OF THE INVENTION

- [0009] A summary of several example embodiments of the disclosure follows. This summary is provided for the convenience of the reader to provide a basic understanding of such embodiments and does not wholly define the breadth of the disclosure. This summary is not an extensive overview of all contemplated embodiments, and is intended to neither identify key or critical elements of all embodiments nor to delineate the scope of any or all aspects. Its sole purpose is to present some concepts of one or more embodiments in a simplified form as a prelude to the more detailed description that is presented later. For convenience,

the term “some embodiments” may be used herein to refer to a single embodiment or multiple embodiments of the disclosure.

[0010] Certain embodiments disclosed herein include a method for streaming real-time data from a user device to a dispatch unit terminal, where the method includes: identifying a connection between a user device and a call center; sending a link to the user device, wherein the link includes instructions to initiate streaming of real-time data from the user device, and further includes a unique identifier associated with the user device; and sending the real-time data to a dispatch unit terminal, where the unique identifier is used to match the real-time data with the dispatch terminal used in the connection.

[0011] Certain embodiments disclosed herein also include a non-transitory computer readable medium having stored thereon instructions for causing a processing circuitry to perform a process, the process comprising: identifying a connection between a user device and a call center; sending a link to the user device, wherein the link comprises instructions to initiate streaming of real-time data from the user device, and further comprises a unique identifier associated with the user device; sending the real-time data to a dispatch unit terminal, wherein the unique identifier is used to match the real-time data with the dispatch terminal used in the connection.

[0012] Certain embodiments disclosed herein also include a system for streaming real-time data from a user device to a dispatch unit terminal, comprising: a processing circuitry; and a memory, the memory containing instructions that, when executed by the processing circuitry, configure the system to: identify a connection between a user device and a call center; send a link to the user device, wherein the link comprises instructions to initiate streaming of real-time data from the user device, and further comprises a unique identifier associated with the user device; send the real-time data to a dispatch unit terminal, wherein the unique identifier is used to match the real-time data with the dispatch terminal used in the connection.

[0013] Certain embodiments disclosed herein also include a method implemented via execution of computing instructions configured to run at one or more processors. The method comprises obtaining a phone number of a mobile device used by a user

making an emergency call. The emergency call is conducted with a recipient through a first connection. The method also comprises transmitting a uniform resource locator (URL) to the mobile device through an electronic message. The electronic message is transmitted through a second connection using the phone number. The second connection is different from the first connection. The electronic message allows the user to click on the URL to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device. The URL is associated with the phone number of the mobile device. The method additionally comprises receiving the real-time video stream from the mobile device through the WebRTC session. The method further comprises sending the real-time video stream to the recipient for display on a screen of the recipient. The real-time video stream is associated with a unique identifier for the mobile device.

[0014] Certain embodiments disclosed herein also include a system comprising processing circuitry and a non-transitory computer-readable medium storing computing instructions that, when executed on the processing circuitry, cause the processing circuitry to perform certain acts. The acts comprise obtaining a phone number of a mobile device used by a user making an emergency call. The emergency call is conducted with a recipient through a first connection. The acts also comprise transmitting a uniform resource locator (URL) to the mobile device through an electronic message. The electronic message is transmitted through a second connection using the phone number. The second connection is different from the first connection. The electronic message allows the user to click on the URL to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device. The URL is associated with the phone number of the mobile device. The acts additionally comprise receiving the real-time video stream from the mobile device through the WebRTC session. The acts further comprise sending the real-time video stream to the

recipient for display on a screen of the recipient. The real-time video stream is associated with a unique identifier for the mobile device.

[0015] Certain embodiments disclosed herein also a non-transitory computer-readable medium storing computing instructions that, when executed on processing circuitry, cause the processing circuitry to perform certain acts. The acts comprise obtaining a phone number of a mobile device used by a user making an emergency call. The emergency call is conducted with a recipient through a first connection. The acts also comprise transmitting a uniform resource locator (URL) to the mobile device through an electronic message. The electronic message is transmitted through a second connection using the phone number. The second connection is different from the first connection. The electronic message allows the user to click on the URL to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device. The URL is associated with the phone number of the mobile device. The acts additionally comprise receiving the real-time video stream from the mobile device through the WebRTC session. The acts further comprise sending the real-time video stream to the recipient for display on a screen of the recipient. The real-time video stream is associated with a unique identifier for the mobile device.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0016] The subject matter disclosed herein is particularly pointed out and distinctly claimed in the claims at the conclusion of the specification. The foregoing and other objects, features, and advantages of the disclosed embodiments will be apparent from the following detailed description taken in conjunction with the accompanying drawings.

[0017] Figure 1 is a network diagram of the system for streaming real-time data according to an embodiment.

[0018] Figure 2 is a sequence diagram illustrating the method according to an embodiment.

[0019] Figure 3 is a flowchart of the method used by the system for streaming real-time data according to an embodiment.

DESCRIPTION OF SPECIFIC EMBODIMENTS OF THE INVENTION

[0020] It is important to note that the embodiments disclosed herein are only examples of the many advantageous uses of the innovative teachings herein. In general, statements made in the specification of the present application do not necessarily limit any of the various claimed embodiments. Moreover, some statements may apply to some inventive features but not to others. In general, unless otherwise indicated, singular elements may be in plural and vice versa with no loss of generality. In the drawings, like numerals refer to like parts through several views.

[0021] By way of example, some disclosed embodiments include a method and system for streaming real-time data from a user device to a call center. The method includes identifying a first connection between a user device and a call center, such as a public-safety answering point (PSAP) for reporting on an emergency or non-emergency incident. The reporting may be a call initiated between the call center and use device. Both the user device and the call center are identified, and a link, such as a uniform resource locator (URL), that includes an identifier unique to the user device is sent to the user device. Upon identification that the link was engaged, the user device is configured to initiate the uploading of streaming real-time data from the user device to the call center. In an embodiment, the uploaded real-time data is associated with the user device using the identifier. The uploading of data may be accomplished by a preinstalled application, or an instant application, on the user device, as explained herein. The real-time data may be forwarded to a first dispatch unit terminal (DUT). According to optional embodiment, the first DUT receives the real-time data and associates the received data with at least an audio content received over the first connection.

[0022] Fig. 1 shows an exemplary diagram of a networked system 100 utilized to describe the various disclosed embodiments. The system 100 includes a network 110 which enables communication between the different elements of the system 100 that are

connected to the network 110. The network 110 may include a cellular network, such as a third or fourth generation cellular network, e.g., the Global System for Mobile Communications (GSM) network, the Enhanced Data rates for GSM Evolution (EDGE) network, the Universal Mobile Telecommunications Service (UMTS) network, the Long-Term Evolution (LTE) network, LTE Advanced network, and the like.

[0023] The system 100 further includes a server 120 that is connected to the network 110. The server 120 contains a hardware and a software component configured to execute predetermined computing tasks, and includes a processing circuitry 123 and a memory 125. The processing circuitry 123 may be realized as one or more hardware logic components and circuits. For example, and without limitation, illustrative types of hardware logic components that can be used include field programmable gate arrays (FPGA s), application-specific integrated circuits (ASICs), application-specific standard products (ASSPs), system-on-a-chip systems (SOCs), general-purpose microprocessors, microcontrollers, digital signal processors (DSPs), and the like, or any other hardware logic components that can perform calculations or other manipulations of information.

[0024] The memory 125 is configured to store software. Software shall be construed broadly to mean any type of instructions, whether referred to as software, firmware, middleware, microcode, hardware description language, or otherwise. Instructions may include code (e.g., in source code format, binary code format, executable code format, or any other suitable format of code). The instructions, when executed, cause the processing circuitry 123 to perform the various processes described herein.

[0025] One or more user devices (UD) 130, are connected to the network 110, i.e., UD 130-1 through 130-n, where 'n' is an integer equal to or greater than 1. The UD 130 may be, for example, a smartphone, a mobile phone, a laptop, a tablet computer, a wearable computing device, and the like. The UD 130 may be configured to collect and upload data and real-time data captured by the UD 130, including, but not limited to, audio data, video data, location data and the like. Additionally, the UD

130 may connect to the network 110 using voice calls as well as voice over internet protocol (VOIP).

[0026] Also connected to the network 110 are one or more call centers 135, i.e. call center 135-1 through call center 135-z where 'z' is an integer equal to or greater than 1. A call center 135 may be, for example, a public-safety answering point (PSAP) that is configured to receive calls made by citizens regarding emergency or non-emergency situations. The PSAP routes the calls to a suitable dispatch unit, such as a dispatch unit terminal (DUT) 140 associated with a particular type of incident.

[0027] A DUT 140, i.e. DUT 140-1 through DUT 140-m (where 'm' is an integer equal to or greater than 1), is an electronic end-point device for receiving emergency and non-emergency calls, live streaming data, data related to the UD 130, and the like. For example, the call center 135 may forward a call to a fire department's DUT for a call regarding a fire, or a police's DUT for a call regarding a criminal act. The DUTs 140 may be connected to the network 110 directly, or via the call center 134.

[0028] The system 100 further includes a database 150 connected to the network 110. Alternatively, the database 150 may be connected directly to the server 120 (not shown). The database 150 may be a data warehouse, a cloud database, and the like, designed to store therein data sent by, for example, the UD 130. The database may further be configured to be accessed by various other components of the system 100, including the call center 135 and the DUT 140.

[0029] According to an embodiment, the server 120 is configured to detect an establishment or an attempted establishment of a first connection between a UD 130 and a call center 135. The first connection may be, for example, a voice call over a cellular network, such as a when a phone call is established between the user device and a call center. For example, the UD 130 may be used to call an emergency response number, e.g., 9-1-1, via a cellular network. When the call is received at a call center 135, a first connection is established. An attempt to establish a connection is determined when a call from a UD 130 is queued. In an additional embodiment, the call is forwarded to a suitable DUT 140, and the server is configured to detect when a first connection is established between a UD 130 and

a DUT 140, e.g., after the call center 135 routes a call from a UD 130 to an appropriate DUT 140.

[0030] In an embodiment, the server 120 is configured to detect the establishment or an attempted establishment of a first connection through an application programming interface (API) of a private branch exchange (PBX) of the call center 135. Through the API, the server 120 can search for an established (or queued) connection, and identify UDs 130 connected to a call center 135. The identification of a UD 130 may be based on its phone number or other unique parameters associated with the UD 130.

[0031] Upon identification of the UD 130 and the call center 135 and/or the DUT 140, the server 120 is configured to send an electronic message to the UD 130 over a second connection over the network 110. The second connection is directly established between the server 120 and a UD 130 over the network 110. The electronic message may be, for example, a short message service (SMS), an MMS, an electronic mail (email) message, and the like. The electronic message includes at least a link that includes an identifier unique to the UD 130. The identifier may be, for example, a code snippet, a randomly generated string, a signature, and so on. Each identifier is uniquely generated for each UD 130 and therefore distinguishes any data sent from different UDs. The link may be, for example, a URL where the unique identifier may be the suffix of the URL, referencing a web address of the call center connected to the UD.

[0032] When the link has been engaged on the UD 130, e.g., selected, tapped, or clicked on, the server 120 is configured to launch an application on the UD 130. In an embodiment, the application is a web browser, where the web browser includes an interface for uploading and/or streaming data. In this particular embodiment, the web browser is utilized to upload or stream real-time data collected by the UD 130.

[0033] In another embodiment, the link sent to the UD 130 is configured to launch an instant application. Instant applications, such as Google® Android Instant Apps, allow users to run applications instantly, without requiring a user to download and install a full application file. The instant application enables the UD 130 to rapidly

open a designated application, such as an emergency application, and start uploading and/or streaming real-time data to the call center 135 (referenced in the link) without requiring any specialized application to be installed on the UD 130 beforehand. For example, when the link is engaged, only the necessary parts of an application's code are downloaded that enable the UD 130 to rapidly stream real-time data. By using an instant application, significant and often critical time is saved, as an instant application can be downloaded and launched more quickly than a full application, thus allowing a UD 130 to begin streaming the real-time data quickly.

[0034] Real-time data may include video, audio, and images captured by the UD 130, text messages, chats, location data and the like. In another embodiment, the real-time data further includes GPS coordinates and/or indoor coordinates. The GPS coordinates may be provided by a GPS receiver installed in the UD 130. The indoor coordinates may be determined using Wi-Fi signals or other RF signals. In an embodiment, a request for using at least one media-capturing component of the UD 130 is included in the link. For example, the link may initiate the real-time streaming of just audio data, or just video data, to the call center 135.

[0035] According to an embodiment, streaming the real-time data is achieved using a Web Real-Time Communication (WebRTC) API that enables real-time communication over peer-to-peer connections. When initiating the web browser on the UD 130 to stream data to the call center 135 and/or to the DUT 140, the server 120 may cause the UD 130 to establish a WebRTC session using a WebRTC API that would allow streaming real-time data from the UD 130 to the call center 135 and/or the DUT 140. WebRTC protocol typically includes the ability to connect two devices without requiring an intermediate server, thereby allowing for data to stream directly without requiring an intermediate server.

[0036] According to another embodiment, some or all portions of the streaming data, such as the location of the UD 130, audio data, and the like, may be sent using other communication protocols, such as hypertext transfer protocol (HTTP), WebSocket, and so on.

- [0037] In some embodiments, the real-time data is streamed from the UD 130 to a server, such as the server 120, in order to first convert the real-time data collected by the UD 130 into a format more suitable for streaming on a DUT 140. The conversion allows the end point devices of the call center 135 to receive, identify and use the real-time data sent initially from the UD 130 through the server 120. The server 120 is configured to send the converted real-time data to the call center 135 or directly to the DUT 140.
- [0038] Any real-time data streamed or otherwise uploaded to the call center 135 is coupled with the unique identifier included in the link. In an embodiment where the real-time data is streamed to the call center 135, after the call center 135, e.g. a PSAP, receives the real-time data with the identifier, the call center 135 routes the received real-time data to a DUT 140 to which the UD 130 was connected to through the first connection.
- [0039] According to an embodiment, the real-time data is associated, at the first DUT 140, with at least an audio content that was received over the first connection. That is, when the real-time data is sent to the first DUT 140, the identifier that was included within the link is utilized for associating the real-time data with the at least audio content at the first DUT 140. In an alternative embodiment, the real-time data is sent from the UD 130 directly to the DUT 140 that it was connected to over the first connection.
- [0040] Fig. 2 is a sequence diagram illustrating the method 200 according to an embodiment. As a non-limiting example, a call is initiated from a user device 130, e.g., a user dials 9-1-1 to report a robbery, and is first connected to a call center 135. The call is then forwarded to an appropriate DUT 140. When the call is answered, or while still in queue, by the DUT 140, the server 120 identifies the UD 130 and sends a link over a second connection, such as an SMS, to the UD 130. When the user engages the link, a web browser is launched, enabling the streaming of real-time data, such as video, audio, location data, and the like, from the UD 130 to the call center 135. The call center then forwards the real-time data to the DUT 140.

- [0041] In an alternate embodiment, the real-time data is sent directly to the DUT 140. In a further embodiment, as further described herein above, the real-time data may be initially converted by the server 120 or a different proxy server (not shown) that is configured to convert the data from the UD 130 into a format that is optimized for the DUT 140 to review and analyze the data. After the conversion, the data is sent to the DUT 140.
- [0042] In an embodiment, the server 120 is further configured to launch an application on the DUT 140 that is designed to display the streamed real-time data from the UD 130. The application may be, for example, a video player through which the real-time data is displayed and may enable a dispatch operator operating the DUT 140 to have a better perspective of the circumstances where the UD 130 is located.
- [0043] According to another embodiment, the server 120 may be configured to use the identification of the UD 130, using for example, the phone number of the UD 130, to extract information associated with the user of the UD 130. The information may be related to, for example, the user's name, sensitivities to certain medications, blood type, disabilities, and so on. The information may be extracted from at least one source, such as the database 150, a web source, and the like, and sent to the DUT 140 together with the real-time data, such that the dispatch operator of the DUT 140 may be able to receive the additional information related to the user.
- [0044] According to another embodiment, the system 100 may be used by one user to assist another user. For example, a first user associated with a first UD 130-1 may contact the call center 135 to report that a second user associated with a second UD 130-2 requires assistance. The first UD 130-1 may provide an identifier for the second UD 130-2, such as a phone number. The identifier of the second UD 130-2 may be received by the server 120, where the server 120 is configured to send a link to the second UD 130-2 over a second connection to initiate streaming of real-time data from the second UD 130-2.
- [0045] According to yet a further embodiment, the system 100 may be utilized for reestablishing a connection between a UD 130 and the call center 135, or a specific DUT 140, upon identification that the connection was lost. For example, a first

connection between a first UD 130-1 and a call center 135 is identified, and after a while the connection is lost. The server 120 uses the identifier, i.e. the phone number, associated with the first UD 130-1, for reestablishing the first connection with the first UD 130-1, and sends, over a second connection, a link to the first UD 130-1 in order to initiate streaming of real-time data from the first UD 130-1.

[0046] Fig. 3 is a flowchart of the method 300 used by the system for streaming real-time data according to an embodiment. At S310, the operation starts by identifying the establishment of a first connection between a user device and a call center. The first connection may pass over a network, such as a cellular or mobile network. For example, the first connection may include a voice call or a VOIP call from a user device, such as a smartphone, to a call center, such as a PSAP. The call center determines what the nature of the call is, such as reporting a fire, a crime, a medical emergency, and the like.

[0047] At S320, the user device is further connected to a dispatch unit terminal that is suitable for the situation. For example, the dispatch unit terminal would be connected to a fire station if the scenario involves a fire, and a police station if the scenario involves a crime. Further, the user device is identified. The identification may be achieved by identifying a phone number or other unique identifier associated with the user device.

[0048] At S330, based on the identification of the user device, and the specific dispatch unit terminal to which it has been connected over the first connection, a link is sent to the user device over a second connection as further described herein above with respect of Figs. 1 and 2. The link includes an identifier unique to the UD 130, and an instruction set to begin streaming data from the user device.

[0049] At S340, based on determination of whether the link was engaged on the user device, e.g., tapped, selected, clicked on, and the like, an application is launched that includes an interface for streaming real-time data collected by the user device. The collection of data may include video or images from a camera, audio from a microphone, location data from a global positioning system, movement from an

accelerometer, detected radio frequency signals, and the like. The real-time data is further associated with the user device by a unique identifier.

[0050] In an embodiment, the application that is launched is a web browser, namely an application primarily designed to display web pages from the internet. As many browser applications have native support for the uploading of real-time data, such as audio recordings, images, video and the like, the browser is capable of initiating and carrying out the streaming of data. Further, as most commonly used user devices, such as smartphones, tablets, personal computers and so on, come pre-installed with a browser application, there is no need to require additional downloading and installation of a specialized application, thus ensuring increased compatibility.

[0051] In a further embodiment, the application includes an instant application, which is reduced version of a full application. An instant application can be initiated from within a browser when activated by a link, and involves downloading only portions of the application that are necessary for the desired task. Further, instant applications do not require a traditional installation on a user device. For example, while a full streaming application would require access to an application marketplace, and account associated with that marketplace, and the completion of a full installation, an instant application can be launched automatically, after only downloading a reduced version of the application, without requiring access to or an account associated with an application marketplace.

[0052] At optional S350, the real-time data is first forwarded to a server, where it is converted into a format that is optimized to allow for quicker streaming of the user device data to the dispatch unit terminal. A unique identifier is associated with the real-time data, allowing the dispatch unit terminal to associate the data with the user device, even if the streaming is accomplished over a second or third connection.

[0053] At S360, the real-time data is uploaded and sent to the dispatch unit. In an embodiment, a peer to peer connection is established between the user device and the call center, where the real-time data is further forwarded to the dispatch unit terminal. In another embodiment, a direct peer to peer connection is established

between the user device and the dispatch unit terminal, where the real-time data is directly uploaded without an intermediary step.

[0054] The streaming real-time data may be transmitted to the dispatch unit terminal using the WebRTC (Web Real-Time Communication) protocol, which allows for real-time communication and transfer of audio, video, and other data directly from within a browser, without requiring the installation of a separate application. WebRTC can be used with many widely used browsers, both in mobile format (e.g., on a smartphone or a tablet), and desktop format (e.g., on a desktop or laptop computer). WebRTC employs APIs that can be executed over multiple platforms, e.g., over Windows®, Android®, iOS® and Linux® without requiring rewriting any of the code. Thus, a link to run browser for streaming real-time data can be executed over a variety of platforms without having to tailor the streaming procedure by individual device. This ensures expanded compatibility allowing for many user devices to successfully stream data.

[0055] As used herein, the phrase “at least one of” followed by a listing of items means that any of the listed items can be utilized individually, or any combination of two or more of the listed items can be utilized. For example, if a system is described as including “at least one of A, B, and C,” the system can include A alone; B alone; C alone; A and B in combination; B and C in combination; A and C in combination; or A, B, and C in combination.

[0056] The various embodiments disclosed herein can be implemented as hardware, firmware, software, or any combination thereof. Moreover, the software is preferably implemented as an application program tangibly embodied on a program storage unit or computer readable medium consisting of parts, or of certain devices and/or a combination of devices. The application program may be uploaded to, and executed by, a machine comprising any suitable architecture. Preferably, the machine is implemented on a computer platform having hardware such as one or more central processing units (“CPUs”), a memory, and input/output interfaces. The computer platform may also include an operating system and microinstruction code. The various processes and functions described herein may be either part of

the microinstruction code or part of the application program, or any combination thereof, which may be executed by a CPU, whether or not such a computer or processing circuitry is explicitly shown. In addition, various other peripheral units may be connected to the computer platform such as an additional data storage unit and a printing unit. Furthermore, a non-transitory computer readable medium is any computer readable medium except for a transitory propagating signal.

[0057] All examples and conditional language recited herein are intended for pedagogical purposes to aid the reader in understanding the principles of the disclosed embodiment and the concepts contributed by the inventor to furthering the art, and are to be construed as being without limitation to such specifically recited examples and conditions. Moreover, all statements herein reciting principles, aspects, and embodiments of the disclosed embodiments, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future, i.e., any elements developed that perform the same function, regardless of structure.

[0058] It is the intent of the Applicant(s) that all publications, patents and patent applications referred to in this specification are to be incorporated in their entirety by reference into the specification, as if each individual publication, patent or patent application was specifically and individually noted when referenced that it is to be incorporated herein by reference. In addition, citation or identification of any reference in this application shall not be construed as an admission that such reference is available as prior art to the present invention. To the extent that section headings are used, they should not be construed as necessarily limiting. In addition, any priority document(s) of this application is/are hereby incorporated herein by reference in its/their entirety.

CLAIMS

What is claimed is:

1. A method implemented via execution of computing instructions configured to run at one or more processors, the method comprising:
 - obtaining a phone number of a mobile device used by a user making an emergency call, wherein the emergency call is conducted with a recipient through a first connection;
 - transmitting a uniform resource locator (URL) to the mobile device through an electronic message, wherein the electronic message is transmitted through a second connection using the phone number, wherein the second connection is different from the first connection, wherein the electronic message allows the user to click on the URL to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device, and wherein the URL is associated with the phone number of the mobile device;
 - receiving the real-time video stream from the mobile device through the WebRTC session; and
 - sending the real-time video stream to the recipient for display on a screen of the recipient, wherein the real-time video stream is associated with a unique identifier for the mobile device.
2. The method of claim 1, wherein the recipient is at least one of an emergency call center or a dispatch unit.
3. The method of claim 1, wherein at least one of:
 - the first connection is a voice call over a cellular network;
 - the electronic message is a text message; or
 - the second connection is a text messaging service.
4. The method of claim 1, wherein the unique identifier comprises the phone number of the mobile device.

5. The method of claim 1, wherein the real-time video stream is transmitted from the mobile device to the recipient through a server that is separate from the mobile device and the recipient.
6. The method of claim 5, wherein the server is a proxy server configured to convert a data format of the real-time video stream.
7. The method of claim 1, wherein the WebRTC session further transmits at least one of (i) GPS location data of the mobile device for display on the screen of the recipient or (ii) one or more photographs taken on the mobile device for display on the screen of the recipient.

8. A system comprising:
- processing circuitry; and
 - a non-transitory computer-readable medium storing computing instructions that, when executed on the processing circuitry, cause the processing circuitry to perform:
 - obtaining a phone number of a mobile device used by a user making an emergency call, wherein the emergency call is conducted with a recipient through a first connection;
 - transmitting a uniform resource locator (URL) to the mobile device through an electronic message, wherein the electronic message is transmitted through a second connection using the phone number, wherein the second connection is different from the first connection, wherein the electronic message allows the user to click on the URL to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device, and wherein the URL is associated with the phone number of the mobile device;
 - receiving the real-time video stream from the mobile device through the WebRTC session; and
 - sending the real-time video stream to the recipient for display on a screen of the recipient, wherein the real-time video stream is associated with a unique identifier for the mobile device.
9. The system of claim 8, wherein the recipient is at least one of an emergency call center or a dispatch unit.
10. The system of claim 8, wherein at least one of:
- the first connection is a voice call over a cellular network;
 - the electronic message is a text message; and
 - the second connection is a text messaging service.

11. The system of claim 8, wherein the unique identifier comprises the phone number of the mobile device.
12. The system of claim 8, wherein the real-time video stream is transmitted from the mobile device to the recipient through a server that is separate from the mobile device and the recipient.
13. The system of claim 12, wherein the server is a proxy server configured to convert a data format of the real-time video stream.
14. The system of claim 8, wherein the WebRTC session further transmits at least one of (i) GPS location data of the mobile device for display on the screen of the recipient or (ii) one or more photographs taken on the mobile device for display on the screen of the recipient.

15. A non-transitory computer-readable medium storing computing instructions that, when executed on processing circuitry, cause the processing circuitry to perform:
- obtaining a phone number of a mobile device used by a user making an emergency call, wherein the emergency call is conducted with a recipient through a first connection;
 - transmitting a uniform resource locator (URL) to the mobile device through an electronic message, wherein the electronic message is transmitted through a second connection using the phone number, wherein the second connection is different from the first connection, wherein the electronic message allows the user to click on the URL to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device, and wherein the URL is associated with the phone number of the mobile device;
 - receiving the real-time video stream from the mobile device through the WebRTC session; and
 - sending the real-time video stream to the recipient for display on a screen of the recipient, wherein the real-time video stream is associated with a unique identifier for the mobile device.
16. The non-transitory computer-readable medium of claim 15, wherein the recipient is at least one of an emergency call center or a dispatch unit.
17. The non-transitory computer-readable medium of claim 15, wherein at least one of:
- the first connection is a voice call over a cellular network;
 - the electronic message is a text message; or
 - the second connection is a text messaging service.
18. The non-transitory computer-readable medium of claim 15, wherein the unique identifier comprises the phone number of the mobile device.
19. The non-transitory computer-readable medium of claim 15, wherein:

the real-time video stream is transmitted from the mobile device to the recipient through a server that is separate from the mobile device and the recipient; and the server is a proxy server configured to convert a data format of the real-time video stream.

20. The non-transitory computer-readable medium of claim 15, wherein the WebRTC session further transmits at least one of (i) GPS location data of the mobile device for display on the screen of the recipient or (ii) one or more photographs taken on the mobile device for display on the screen of the recipient.

**SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING
REAL-TIME DATA FROM A USER DEVICE**

ABSTRACT

A method comprising obtaining a phone number of a mobile device used by a user making an emergency call. The emergency call is conducted with a recipient through a first connection. The method also comprises transmitting a uniform resource locator (URL) to the mobile device through an electronic message. The electronic message is transmitted through a second connection using the phone number. The second connection is different from the first connection. The electronic message allows the user to click on the URL to access a web browser on the mobile device, instead of a full application on the mobile device, to establish a WebRTC (Web Real-Time Communication) session to transmit a real-time video stream from the mobile device. The URL is associated with the phone number of the mobile device. The method additionally comprises receiving the real-time video stream from the mobile device through the WebRTC session. The method further comprises sending the real-time video stream to the recipient for display on a screen of the recipient. The real-time video stream is associated with a unique identifier for the mobile. Other embodiments are described.

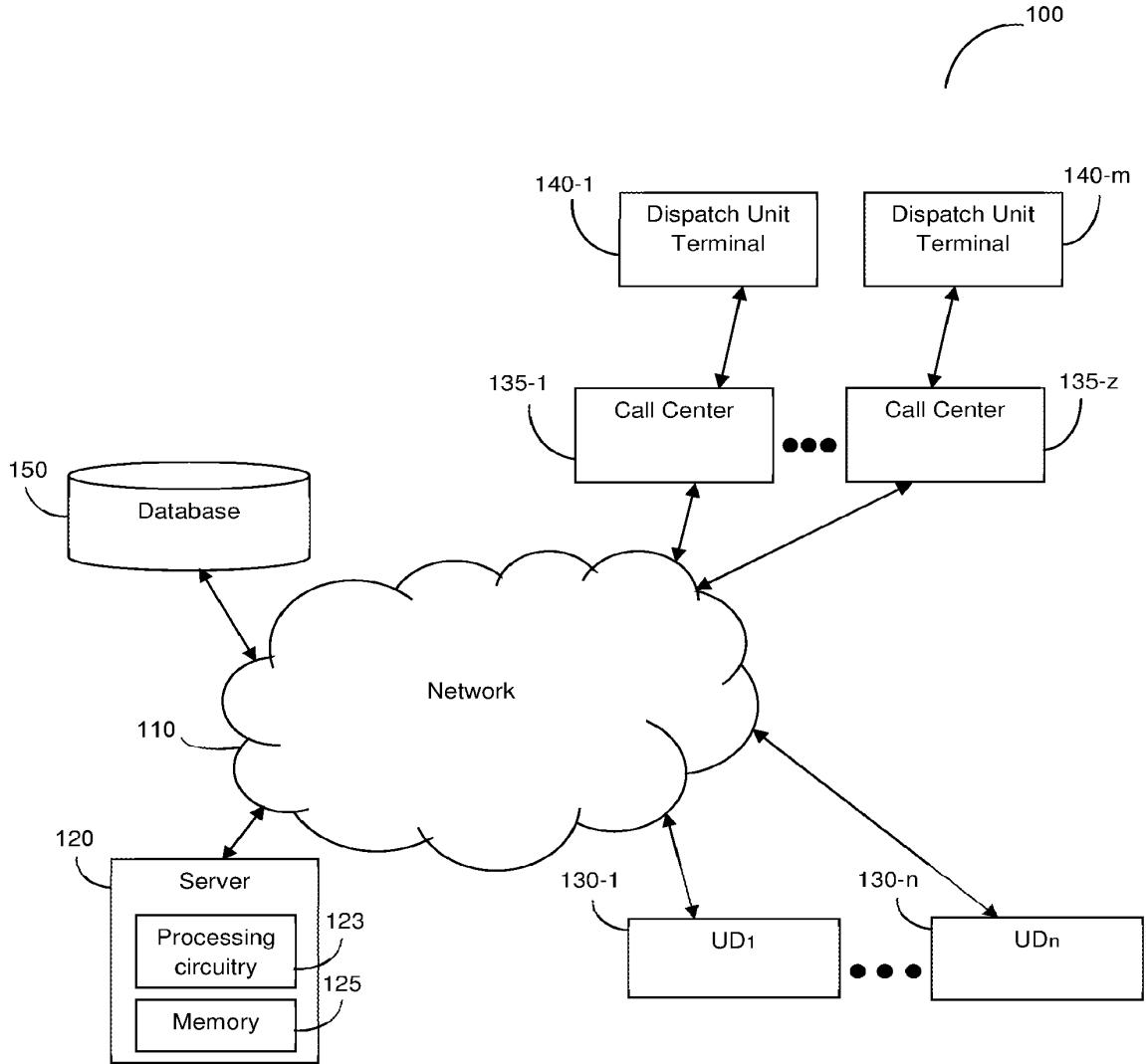


FIG. 1

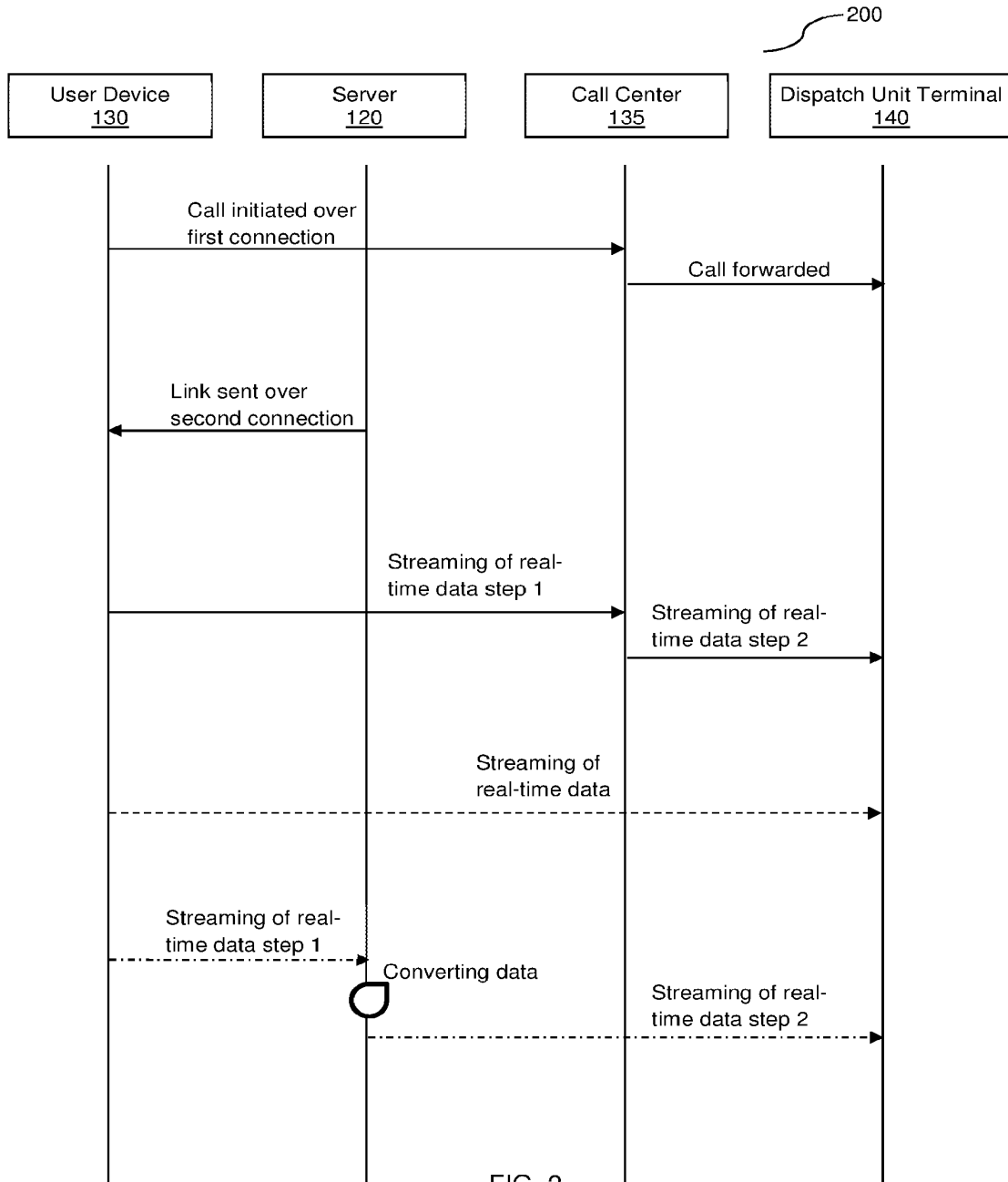


FIG. 2

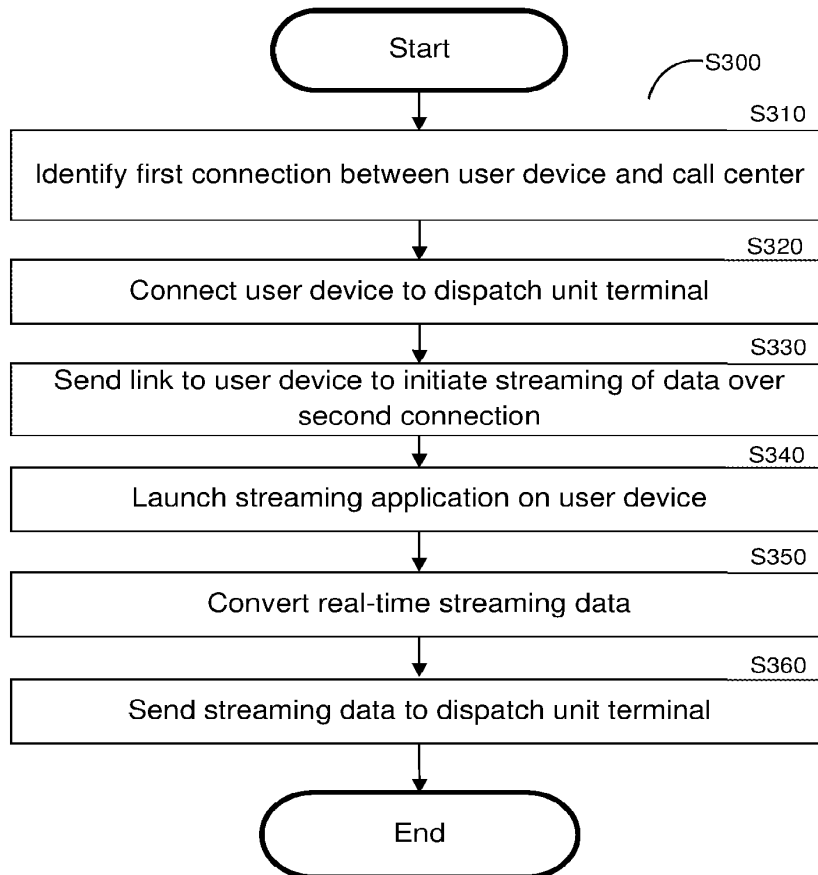


FIG. 3

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE			
First Named Inventor/Applicant Name:	Alexander Dizengof			
Filer:	Cory Smith/Lisa Mansur			
Attorney Docket Number:	3010043.1			
Filed as Small Entity				
Filing Fees for Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
UTILITY FILING FEE (ELECTRONIC FILING)	4011	1	80	80
UTILITY SEARCH FEE	2111	1	350	350
UTILITY EXAMINATION FEE	2311	1	400	400
REQUEST FOR PRIORITIZED EXAMINATION	2817	1	2100	2100
Pages:				
Claims:				
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
PROCESSING FEE, EXCEPT PROV. APPLS.	2830	1	70	70
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				3000

Electronic Acknowledgement Receipt

EFS ID:	46607915
Application Number:	17943956
International Application Number:	
Confirmation Number:	2316
Title of Invention:	SYSTEM, METHOD, AND COMPUTER-READABLE MEDIUM FOR STREAMING REAL-TIME DATA FROM A USER DEVICE
First Named Inventor/Applicant Name:	Alexander Dizengof
Customer Number:	46019
Filer:	Cory Smith/Lisa Mansur
Filer Authorized By:	Cory Smith
Attorney Docket Number:	3010043.1
Receipt Date:	13-SEP-2022
Filing Date:	
Time Stamp:	17:34:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	\$3000
RAM confirmation Number	E20229CH35363793
Deposit Account	024467
Authorized User	Lisa Mansur

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)
 37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Track One Request	3010043-000001-Track-1-Request-for-Prioritized-Examination.pdf	135163	no	2
			9fe38a2555e32d85c6d270a7804f097063ec5ae3		
Warnings:					
Information:					
2	Application Data Sheet	3010043-000001-Application-Data-Sheet.pdf	2231640	no	8
			bab2ef39832074c08b70e75ab429a5efc7273458		
Warnings:					
Information:					
3	Oath or Declaration filed	3010043-000001-Declaration-Dizengof.pdf	162643	no	2
			5be4af52b92c323050ea46c5b98a9c2c869c1e00		
Warnings:					
Information:					
4		3010043-000001-Patent-Application.pdf	211636	yes	24
			4433173586f0935fc09c1d05b97ff238f34b8157		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	17	
	Claims		18	23	
	Abstract		24	24	
Warnings:					
Information:					
5	Drawings-other than black and white line drawings	3010043-000001-Drawings.PDF	33240	no	3
			45ff6a3f5ea89f428ffc289a938d28bd3e352967		

Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	50834	no	2
			136788feba198de64f5fa5708d68374c76e5a7a3		
Warnings:					
Information:					
Total Files Size (in bytes):				2825156	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

SCORE Placeholder Sheet for IFW Content

Application Number: 17943956

Document Date: 09/13/2022

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access SCORE content via DAV or via the SCORE web page.
- External customers may access SCORE content via PAIR using the Supplemental Content tab.