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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/603,252	10/07/2019	Yoseph KOREN	09708-P0001A

CONFIRMATION NO. 6147

49443
Pearl Cohen Zedek Latzer Baratz LLP
7 Times Square
19th Floor
New York, NY 10036

POA ACCEPTANCE LETTER

OC000000080756709

Date Mailed: 11/19/2024

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/11/2024.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth 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**.

/sltorres/

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/603,252	10/07/2019	Yoseph KOREN	09708-P0001A

CONFIRMATION NO. 6147

136531
The Roy Gross Law Firm, LLC
101 Merritt 7
Suite 300
Norwalk, CT 06851

POWER OF ATTORNEY NOTICE

OC000000080756685

Date Mailed: 11/19/2024

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/11/2024.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth 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**.

/sltorres/

UNITED STATES
PATENT AND TRADEMARK OFFICE

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

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
16/603,252	**11/11/2024 02:02:59 AM Z ET**	**09708-P0001A**

Title of Invention

SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

Application Information

APPLICATION TYPE	Utility - U.S. National Stage under 35 USC 371	PATENT #	11106824
CONFIRMATION #	6147	FILED BY	Einav Ofek Cohen
PATENT CENTER #	67907921	FILING DATE	10/07/2019
CUSTOMER #	136531	FIRST NAMED INVENTOR	Yoseph KOREN
INTL. APPLICATION #	-	INTL. FILING DATE	-
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Caleb Pollack

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
P-566702-US-U-REVPOA-07NOV24.pdf	2	Power of Attorney	164 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
P-566702-US-U-REVPOA-07NOV24.pdf	B37615F224215685AC0A656695B87E5507BAF1607AD1C0471AC5FEA23675B6AB6DDE4F1748357A695B9D141E58739CBBC607B73B6E638E42B2BF71DB7F221BED

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.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
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 displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA/82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	16/603,252
Filing Date	October 07, 2019
First Named Inventor	Yoseph KOREN
Title	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA
Art Unit	2434
Examiner Name	Shams, Mohammads
Attorney Docket Number	P-566702-US

SIGNATURE of Applicant or Patent Practitioner

Signature		Date	7 November 2024
Name	Caleb Pollack	Registration Number	**37,912**
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. 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 3 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.

PTO/AIA/82B (07-13)
Approved for use through 03/31/2021. OMB 0651-0035
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 displays a valid OMB control number.

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☒ I hereby appoint the Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: **49443**

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☒ The address associated with the above-mentioned Customer Number:

OR

☐ The address associated with Customer Number: **49443**

OR

☒ Firm *or* Individual Name	Pearl Cohen Zedek Latzer Baratz LLP				
Address	7 Times Square, 19th Floor				
City	New York	State	NY	ZIP	10036
Country	USA				
Telephone	(646) 878-0800	Email	USPTO@PearlCohen.com		

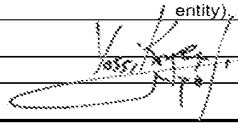
I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

QPrivacy USA LLC

☐ Inventor or Joint Inventor (title not required below)
☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)
☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)
☐ Person Who Otherwise Shows Sufficient Proprietary Interest (*e.g.,* a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date	November 5, 2024
Name	Yossi Koren		
Title	Manager		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. 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 3 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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/603,252	10/07/2019	Yoseph KOREN	P-566702-US

CONFIRMATION NO. 6147

136531
The Roy Gross Law Firm, LLC
101 Merritt 7
Suite 300
Norwalk, CT 06851

POA ACCEPTANCE LETTER

OC000000077787150

Date Mailed: 09/12/2024

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/28/2024.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth 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**.

/snguyen/

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/603,252	10/07/2019	Yoseph KOREN	P-566702-US

CONFIRMATION NO. 6147

49443
Pearl Cohen Zedek Latzer Baratz LLP
7 Times Square
19th Floor
New York, NY 10036

POWER OF ATTORNEY NOTICE

OC000000077787087

Date Mailed: 09/12/2024

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 08/28/2024.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth 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**.

/snguyen/

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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 displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date
Not Yet Known	Herewith

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 136531

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

QPrivacy USA LLC

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	August 28, 2024
Name	Yossi Koren		
Title	Manager		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of oren forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. 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 3 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.

ASSIGNMENT AGREEMENT

This ASSIGNMENT AGREEMENT ("**Assignment Agreement**") is made as of August 28 , 2024 (the "**Effective Date**") by and between: (1) **Privacy Rating Ltd**, a company limited by shares organized under the laws of Israel, company registration number 515765287 (the "**Assignor"**); and (2) **QPrivacy USA LLC**, a limited liability company registered in the State of Texas, USA (the "**Assignee**" and together with the Assignor, the "**Parties**").

WHEREAS, the Parties have executed and delivered that certain Patent Sale Agreement dated as of the Effective Date (the "**Patent Sale Agreement**"); and

WHEREAS, pursuant to Section 1.6 of the Patent Sale Agreement, the Assignor has agreed, as a condition to the consummation of the transactions evidenced by the Agreement, to execute and deliver this Assignment Agreement to the Assignee.

NOW, THEREFORE, in consideration of the consummation of the transactions evidenced by the Patent Sale Agreement, the promises set forth in this Assignment Agreement and for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

1. Assignment of Patents. The Assignor hereby grants, transfers, assigns, sells, conveys and relinquishes exclusively to the Assignee, its successors and assigns forever, on an exclusive basis, the entire title, right, interest, ownership and all subsidiary rights in and to the patents and patent applications (and any continuations thereof after the Effective Date) listed on Exhibit A hereto (the "**Patents**"), and to all of the rights and obligations relating thereto, including, but not limited to, the following, all in connection with the Patents:

(a) the right to sue and recover for, and the right to profits or damages due or accrued arising out of or in connection with, any and all past, present or future infringements of the Patents;

(b) the right to file patent applications and secure patents in the Assignee's own name and to secure renewals, divisionals, continuations (in whole or in part), substitutions, reissues, reexaminations and extensions of such patent applications and/or patents in the United States of America or any other country; and

(c) the right to determine, in the Assignee's sole discretion, whether or not any patent applications or patents, as applicable, shall be filed, preserved, maintained or registered.

2. Power of Attorney. The Assignor does hereby constitute and appoint each of the directors and officers of the Assignee, its successors and assigns, as the Assignor's true and lawful attorney, with full power of substitution for the Assignor, and in its name, place and stead or otherwise, but on behalf of and for the benefit of the Assignee, its successors and assigns, to take all actions and execute all documents on behalf of the Assignor necessary to effect the assignment set forth in Section 1 hereof, and from time to time to institute and prosecute in the Assignor's name or otherwise, but at the direction and expense and for the benefit of the

Assignee and its successors and assigns, any and all proceedings at law, in equity or otherwise, which the Assignee, its successors or assigns may deem proper in order to collect, assert or enforce any claim, right or title of any kind in and to the Patents and to defend and compromise any and all actions, suits and proceedings in respect of any of said Patents and to do any and all such acts and things in relation thereto as the Assignee, its successors or assigns shall deem advisable, the Assignor hereby declaring that the appointment hereby made and the powers hereby granted are coupled with an interest and are and shall be irrevocable by the Assignor in any manner or for any reason.

3. Further Assurances. Upon the request of the Assignee or in case for any reason the Power of Attorney set forth in Section 2 hereof is insufficient to effect the assignment set forth in Section 1 hereof or effect any other purpose set forth in Section 2 hereof, the Assignor agrees for itself and its successors, representatives and assigns, without further compensation, to perform such lawful acts and to sign such further applications, assignments, statements and other lawful documents as the Assignee may reasonably request to effectuate fully the assignment contained in Section 1 hereof and the purposes set forth in Section 2 hereof.

4. Representations and Warranties. The Assignor represents and warrants to the Assignee that: (i) the Assignor owns the Patents free and clear of all liens and encumbrances; (ii) the Assignor has the power and authority to execute this Assignment Agreement; (iii) the Assignor has not entered into any agreement that conflicts with the terms of this Assignment Agreement; (iv) to the Assignor's knowledge, there are no pending or threatened claims by any third party relating to the Patents and/or the use, registration, or ownership of the Patents; and (v) all applicable registration fees for the Patents are paid in full.

5. General. This Assignment Agreement is binding upon and inures to the benefit of the Parties and their respective successors and assigns. This Assignment Agreement and the Patent Sale Agreement set forth the entire agreement between the Parties and supersedes any and all prior or contemporaneous, written or oral agreements with respect to the subject matter hereof. This Assignment Agreement may be amended only in writing executed by each of the Parties. This Assignment Agreement will be governed by the laws of the State of Israel, without regard to its conflict of laws principals.

[Remainder of Page Intentionally Left Blank]

IN WITNESS WHEREOF, the Parties, by their duly authorized representatives, have caused this Assignment Agreement to be executed as of the Effective Date.

Privacy Rating Ltd.

By:_____

Name: Yossi Koren
Title: Co-founder and CEO

QPrivacy USA LLC

By:_____

Name: Yossi Koren
Title: Manager

EXHIBIT A

List of Patents

U.S. Patent No. 11,106,824; System and method for dynamic management of private data; Issued on August 31, 2021

U.S. Patent No. 11,816,249; System and method for dynamic management of private data; Issued on November 14, 2023

U.S. Patent No. 12,013,971; System and method for dynamic management of private data; Issued on June 18, 2024

U.S. Patent Application No. 18/745,488; System and method for dynamic management of private data; Filed on June 17, 2024

PCT Application No. WO2018189736A1; System and method for dynamic management of private data; Filed on March 28, 2018

Israel Patent No. IL251683;System and method for dynamic management of private data; Issued on November 30, 2019

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. 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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: QPrivacy USA LLC

Application No./Patent No.: 11,106,824 Filed/Issue Date: 08/31/2021

Titled: SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

QPrivacy USA LLC, a company

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: inventors To: PRIVACY RATING LTD.

   The document was recorded in the United States Patent and Trademark Office at

   Reel 053825, Frame 0618, or for which a copy thereof is attached.

2. From: PRIVACY RATING LTD. To: QPrivacy USA LLC

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). 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. 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.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. 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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Roy D. Gross/	August 28, 2024
Signature	Date
Roy D. Gross	63,524
Printed or Typed Name	Title or Registration 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.

UNITED STATES
PATENT AND TRADEMARK OFFICE

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

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
16/603,252	**08/28/2024 09:37:32 PM Z ET**	**P-566702-US**

Title of Invention

SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

Application Information

APPLICATION TYPE	Utility - U.S. National Stage under 35 USC 371	PATENT #	11106824
CONFIRMATION #	6147	FILED BY	Roy Gross
PATENT CENTER #	66968638	FILING DATE	10/07/2019
CUSTOMER #	49443	FIRST NAMED INVENTOR	Yoseph KOREN
INTL. APPLICATION #	-	INTL. FILING DATE	-
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	-

Documents

TOTAL DOCUMENTS: 3

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
09708-P0001A-373c-statement.pdf	3	Assignee showing of ownership per 37 CFR 3.73	120 KB
09708-P0001A-US POA SIGNED.pdf	1	Power of Attorney	194 KB
09708-Assignment Agreement Final-SIGNED.pdf	4	Assignee showing of ownership per 37 CFR 3.73	385 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)

09708-P0001A-373c-statement.pdf	4A2A8BCD600AF0DF1C785293A91B20894365DED63830305EF70C7ABC2E81DCB5D4A10E4D4C3C06B2E932B25409AA437761EB8B81E06511F5FF7EB63F5134A291
09708-P0001A-US POA SIGNED.pdf	175FC7DB5A57394E98CA61C904ED73EE5712B46C97608F419A5808897F4A6DAD573F3704BFCD84C5ED66FFB1514B0E2C72A920C415B16FB0BCDCD8CC18465248
09708-Assignment Agreement Final-SIGNED.pdf	F83A13414BD65C8B26ECF810FEA40FE1054E4F853501850F19C4F39A813F2CB7850564BEFF6DE27031A9BA03408EE9219D29112FCF8421ABCA9D8E91E7272FF9

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.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/603,252	08/31/2021	11106824	P-566702-US	6147

49443 7590 08/11/2021

Pearl Cohen Zedek Latzer Baratz LLP
7 Times Square, 19th Floor
New York, NY 10036

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

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 Data Management (ODM) at (571)-272-4200.

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

Yoseph KOREN, Ganey Tikva, ISRAEL;
Privacy Rating Ltd., Ganey Tikva, ISRAEL
Yehonatan WASSERMAN, Kiryat Ono, 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.

IR103 (Rev. 10/09)

PTO/SB/08b (07-09)
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.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	16/603,252
Filing Date	October 07, 2019
First Named Inventor	Yoseph KOREN
Art Unit	2434
Examiner Name	Shams, Mohammads
Attorney Docket Number	P-566702-US

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (where appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	1	ANDERSON et al. "Identifying Encrypted Malware Traffic with Contextual Flow Data" AISec'16, October 28 2016, Vienna, Austria pp. 35-46	☐
			☐
			☐
			☐
			☐
			☐
			☐

Examiner Signature	/MOHAMMAD S SHAMS/	Date Considered	07/26/2021

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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 2 hours 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, 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 (1-800-786-9199) and select option 2.

20 July 2021

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.S.S./

Electronic Patent Application Fee Transmittal

Application Number:	16603252
Filing Date:	07-Oct-2019
Title of Invention:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA
First Named Inventor/Applicant Name:	Yoseph KOREN
Filer:	Caleb Pollack/Laura Saporta
Attorney Docket Number:	P-566702-US

Filed as Small Entity

Filing Fees for U.S. National Stage under 35 USC 371

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:				
UTILITY APPL ISSUE FEE	2501	1	600	600

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**600**

Electronic Acknowledgement Receipt	
EFS ID:	43374456
Application Number:	16603252
International Application Number:	
Confirmation Number:	6147
Title of Invention:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA
First Named Inventor/Applicant Name:	Yoseph KOREN
Customer Number:	49443
Filer:	Caleb Pollack/Laura Saporta
Filer Authorized By:	Caleb Pollack
Attorney Docket Number:	P-566702-US
Receipt Date:	29-JUL-2021
Filing Date:	07-OCT-2019
Time Stamp:	10:49:16
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$600
RAM confirmation Number	E20217SA49571444
Deposit Account	602041
Authorized User	Laura Saporta
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.20 (Post Issuance fees)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	P-566702-US-ISS-FEE-TRANSMITTAL.pdf	63456 bfc94cf22b57397fd80e079a29a19269ee2e56a6	no	4
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	37994 100eb72b0999f07b850b361d7250d83956e88818	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	101450		

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.

PART B – FEE(S) TRANSMITTAL

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

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

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

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

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

49443 7590 04/29/2021

PEARL COHEN ZEDEK LATZER BARATZ LLP
7 TIMES SQUARE, 19TH FLOOR
NEW YORK, NY 10036

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 facsimilie transmitted to the USPTO (571) 273-2885, on the date indicated below.

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/603,252	10/07/2019	Yoseph KOREN	P-566702-US	6147

TITLE OF INVENTION: SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
NONPROVISIONAL	SMALL	$600	$0.00	$0.00	$600	07/29/2021

EXAMINER	ART UNIT	CLASS-SUBCLASS
Shams, Mohammad S	2434	726-009000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

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

1 PEARL COHEN ZEDEK
2 LATZER BARATZ LLP
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: Privacy Rating Ltd.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Ganey-Tikva, 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) ☐ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid issue fee shown above)*
☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)
☒ To the extent any fees due associated with this filing are not paid or not able to be paid by credit card, and to the extent any overpayment is made, the Director is hereby authorized to charge the required fee(s), or credit any overpayment to Deposit Account No. **60-2041**

5. **Change in Entity Status** (from status indicated above)
☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27
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.
☐ Applicant changing to regular undiscounted fee 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 CFR 1.4 for signature requirements and certifications.

Authorized Signature: __/Caleb Pollack/_____ Date: July 29, 2021

Typed or printed name: Caleb Pollack Registration No: 37,912

PTOL-85 Part B (08-18) Approved for use through 01/03/2020 OMB 0651-0033 U.S. Patent and Trademark Office; U.S DEPARTMENT OF COMMERCE

Attorney Docket No.: P-566702-US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	KOREN, Yoseph et al.	Examiner:	Shams, Mohammad S
Serial No.:	16/603,252	Group Art Unit:	2434
Filed:	October 07, 2019	Confirmation No.:	6147
Title:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA		

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

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

Sir/Madam:

Applicant(s) would like to thank the Examiner for the allowance of the subject application based on the distinctions enumerated in the "Statement for Reasons of Allowance". Applicant(s) agree, without prejudice, that these distinctions provide sufficient basis for allowance of the application; however, Applicant(s) respectfully submit that there may be alternative and/or additional patentable distinctions between the claimed invention and the cited prior art, related or unrelated to those explicitly addressed in the "Statement of Reasons for Allowance".

Should the Examiner have any question or comment as to the form, content or entry of this paper, the Examiner is requested to contact the undersigned counsel at the telephone number below.

Respectfully submitted,

/Caleb Pollack/

Caleb Pollack
Attorney/Agent for Applicant(s)
Registration No. 37,912

Dated: July 29, 2021

Pearl Cohen Zedek Latzer Baratz LLP
1500 Broadway, 12th Floor
New York, New York 10036
Tel: (646) 878-0800
Fax: (646) 878-0801

Attorney Docket No.: P-566702-US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	KOREN, Yoseph et al.	Examiner:	Shams, Mohammad S
Serial No.:	16/603,252	Group Art Unit:	2434
Filed:	October 07, 2019	Confirmation No.:	6147
Title:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA		

INTERVIEW SUMMARY

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

Madam/Sir:

On April 13,. 2021 the undersigned spoke with the Examiner by telephone regarding an amendment to claim 24 to result in allowance. Agreement was reached; no prior art was discussed.

No fees are believed to be due in conjunction with this paper. If any such fees are due, please charge any fees associated with this paper to deposit account No. **60-2041.**

Respectfully submitted,

/Caleb Pollack/

Caleb Pollack
Attorney/Agent for Applicant(s)
Registration No. 37,912

Dated: July 29, 2021

Pearl Cohen Zedek Latzer Baratz LLP
7 Times Square, 19th Floor
New York, New York 10036
Tel: (646) 878-0800
Fax: (646) 878-0801

PTO/SB/08b (07-09)
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.

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*				***Complete if Known***	
				Application Number	**16/603,252**
				Filing Date	**October 07, 2019**
				First Named Inventor	**Yoseph KOREN**
				Art Unit	**2434**
(use as many sheets as necessary)				Examiner Name	**Shams, Mohammads**
Sheet	**1**	of	**1**	Attorney Docket Number	**P-566702-US**

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (where appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	1	ANDERSON et al. "Identifying Encrypted Malware Traffic with Contextual Flow Data" AISec'16, October 28 2016, Vienna, Austria pp. 35-46	☐
			☐
			☐
			☐
			☐
			☐
			☐

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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 2 hours 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, 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 (1-800-786-9199) and select option 2.

Electronic Patent Application Fee Transmittal

Application Number:	16603252
Filing Date:	07-Oct-2019
Title of Invention:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA
First Named Inventor/Applicant Name:	Yoseph KOREN
Filer:	Devorah N Livneh/Laura Saporta
Attorney Docket Number:	P-566702-US

Filed as Small Entity

Filing Fees for U.S. National Stage under 35 USC 371

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($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	130	130
		Total in USD ($)		**130**

Electronic Acknowledgement Receipt	
EFS ID:	43291732
Application Number:	16603252
International Application Number:	
Confirmation Number:	6147
Title of Invention:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA
First Named Inventor/Applicant Name:	Yoseph KOREN
Customer Number:	49443
Filer:	Devorah N Livneh/Laura Saporta
Filer Authorized By:	Devorah N Livneh
Attorney Docket Number:	P-566702-US
Receipt Date:	22-JUL-2021
Filing Date:	07-OCT-2019
Time Stamp:	04:51:57
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$130
RAM confirmation Number	E20217L552461831
Deposit Account	602041
Authorized User	Laura Saporta
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 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		P-566702-US-IDS-FORM-20JUL21.pdf	59818 e7967c5edcc2769f792c3f0e2b96db8a619ee3a3	yes	4
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Transmittal Letter		1	3	
	Information Disclosure Statement (IDS) Form (SB08)		4	4	
Warnings:					
Information:					
2	Non Patent Literature	Identifing-Encrypted-Malware-Traffic-with-Contextual-Flow-Data.pdf	762836 2a3775339774 59cd7a9d713d84901add45b012f5	no	12
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30512 12b42cafb9c5c179112b403aa75cc9a1ae60e116	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	853166		

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.

Attorney Docket No.: P-566702-US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Yoseph-IL KOREN et al.	Examiner:	Shams, Mohammads
Serial No.:	16/603,252	Group Art Unit:	2434
Filed:	October 07, 2019	Confirmation No.:	6147
Title:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA		

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

Sir/Madam:

INFORMATION DISCLOSURE STATEMENT

Pursuant to 37 C.F.R. §§1.56, 1.97 and 1.98, this Information Disclosure Statement includes Form PTO/SB/08:

1. ☐ listing documents including patents, publications and other information for consideration by the Examiner, however, since the subject application was filed after June 30, 2003, copies of United States patents and/or United States patent application publications are not included in this information disclosure statement; and/or
2. ☐ listing documents including patents, publications and other information that have been previously cited or submitted to the Patent Office in prior application U.S. Patent application No. , filed which is properly identified and relied on for an earlier effective filing date under 35 U.S.C. 120 for consideration by the Examiner; however, in accordance with 37 C.F.R. 1.98(d), copies of such documents are not included in this information disclosure statement; and/or
3. ☒ listing documents including patents, publications, and other information for consideration by the Examiner, copies of which are included with this information disclosure statement;
4. ☐ listing documents including patents, publications, and other information for consideration by the Examiner, which were cited in a communication from a foreign patent office in a counterpart foreign application, copies of which are included with this information disclosure statement.

The information herein cited is only in fulfillment of Applicant(s) duty of candor in disclosing all information brought to Applicant(s) attention. This submission does not represent that a search has been made or that no better art exists and does not constitute an admission that each or all of the listed documents are material or constitute "prior art". If it should be determined that any of the listed documents do not constitute "prior art" under United States law, Applicant(s) reserve the right to present to the office the relevant facts and law regarding the appropriate status of such documents.

Applicant(s) further reserve(s) the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

In accordance with MPEP Sections 609 and 707.05(b), it is requested that each and every document cited (including any cited in applicant's specification which is not repeated on the attached Form PTO-1449) be given thorough consideration and that it be cited of record in the prosecution history of the present application by initialing on Form PTO-1449. Such initialing is requested even if the Examiner does not consider it to be prior art for any reason, or even if the Examiner does not believe that the guidelines for citation have been fully complied with. This is requested so that each document becomes listed on the face of the patent issuing on the present application and is evidence that the Examiner has considered the document. Neither the submission of the Information Disclosure Statement nor the content of any document cited herein constitutes a disclaimer of claim scope or an admission that any item submitted constitutes prior art.

This Information Disclosure Statement is being filed:

I) ☐ Within three (3) months of filing the subject Application or entry of the subject Application into the national stage; or before mailing of the first Office Action on the merits of the subject Application, whichever event occurs last; or before mailing of the first Office Action on the merits after filing a request for continued examination, pursuant to of 37 C.F.R §1.97 (b); or

II) ☐ After the period specified in (I) but before the mailing date of either a final Official Action under 37 C.F.R §1.113 or a notice of allowance under 37 C.F.R §1.311 whichever occurs first and;

1. ☐ the undersigned hereby states that each item of information listed on the Form PTO-1449 was either (i) cited in a communication from a foreign patent office in a counterpart foreign application not more than three (3) months prior to the filing of this Information Disclosure Statement or (ii) not cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, not known to any individual designated in §1.56(c) more than three (3) months prior to the filing of this information disclosure statement; or

2. ☐ the fee in the amount of $260 (Large Entity) under 37 C.F.R §1.17 (p) is being paid by credit card (note deposit account information below in the event of lack of credit card payment).

III) ☒ After the period in (I) and (II) but before the payment of the issue fee and,

1. The undersigned hereby states:

a) ☐ that each item of information cited on the form PTO-1449 was first cited in a communication from a foreign Patent Office in a counterpart foreign

application not more than three (3) months prior to the filing of this Information Disclosure Statement; or

b) ☒ that no items of information contained in Form PTO-1449 were cited in a communication from a foreign patent office in a counterpart foreign application, and to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement; and

2. ☒ The Petition fee in the amount of $130 (Small Entity) under 37 C.F.R §1.17 is being paid by credit card (note deposit account information below in the event of lack of credit card payment).

To the extent that there are any fees associated with this filing that are due but are not paid or are not able to be paid by a credit card mentioned elsewhere in this document, Applicants authorize the U.S. Patent and Trademark Office to charge any such fees to deposit account No. **60-2041**.

Respectfully submitted,

/Devorah N. Livneh/
Devorah N. Livneh
Attorney/Agent for Applicant(s)
Registration No. 71,347

Dated: July 20, 2021

Pearl Cohen Zedek Latzer Baratz LLP
7 Times Square, 19th Floor
New York, New York 10036
Tel: (646) 878-0800
Fax: (646) 878-0801

PTO/SB/08a (07-09)
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.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	16/603,252
Filing Date	October 07, 2019
First Named Inventor	KOREN, Yoseph
Art Unit	2434
Examiner Name	Shams, Mohammads
Attorney Docket Number	P-566702-US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A	US-9,609,025	Mar. 28, 2017	Betzler Boas et al.	
	B	US-9,477,836	Oct. 25, 2016	Rambam Shishir Krovvidi et al.	
	C	US-2017/098215	Apr. 6, 2017	Brotsky Daniel C	
M.S.S.	D	US-2012/0222083	Aug. 30, 2012	VAHA-SIPLA et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
M.S.S.		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	E	WO 2013 103782	Jul. 11, 2013	3M Innovative Properties Company		☐
	F	WO 2014 031041	Feb. 27, 2014	Ericsson Telefon AB et al.		☐
M.S.S.						☐
						☐
						☐
						☐
						☐
M.S.S.						☐

Examiner Signature	/MOHAMMAD S SHAMS/	Date Considered	01/07/2021

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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 2 hours 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, 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 (1-800-786-9199) and select option 2.

2 December 2020

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.S.S./

PTO/SB/08b (07-09)
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.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	16/603,252
Filing Date	October 07, 2019
First Named Inventor	KOREN, Yoseph
Art Unit	2434
Examiner Name	Shams, Mohammads
Attorney Docket Number	P-566702-US

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (where appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	G	Supplementary European Search Report Application No. EP 18785029 dated Sep. 15, 2020	☐
	H	PCT IPRP International Application No. PCT/IL2018050359. International Filing Date Mar. 28, 2018	☐
M.S.S.			☐
M.S.S.			☐
M.S.S.			☐
M.S.S.			☐
M.S.S.			☐
M.S.S.			☐
M.S.S.			☐
M.S.S.			☐
M.S.S.			☐

Examiner Signature	/MOHAMMAD S SHAMS/	Date Considered	01/07/2021

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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 2 hours 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, 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 (1-800-786-9199) and select option 2.

2 December 2020

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.S.S./

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

49443 7590 04/29/2021

Pearl Cohen Zedek Latzer Baratz LLP
7 Times Square, 19th Floor
New York, NY 10036

EXAMINER	
SHAMS, MOHAMMAD S	
ART UNIT	PAPER NUMBER
2434	

DATE MAILED: 04/29/2021

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/603,252	10/07/2019	Yoseph KOREN	P-566702-US	6147

TITLE OF INVENTION: SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	07/29/2021

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

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

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

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

PART B - FEE(S) TRANSMITTAL

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

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

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

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

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

49443 7590 04/29/2021
Pearl Cohen Zedek Latzer Baratz LLP
7 Times Square, 19th Floor
New York, NY 10036

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

Certificate of Mailing or Transmission

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/603,252	10/07/2019	Yoseph KOREN	P-566702-US	6147

TITLE OF INVENTION: SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	07/29/2021

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHAMS, MOHAMMAD S	2434	726-009000

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

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

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

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

1 _____
2 _____
3 _____

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

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

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

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

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

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

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

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

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

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

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

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/603,252	10/07/2019	Yoseph KOREN	P-566702-US	6147

49443 7590 04/29/2021
Pearl Cohen Zedek Latzer Baratz LLP
7 Times Square, 19th Floor
New York, NY 10036

EXAMINER	
SHAMS, MOHAMMAD S	

ART UNIT	PAPER NUMBER
2434	

DATE MAILED: 04/29/2021

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

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

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

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

PTOL-85 (Rev. 02/11)

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

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

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

Privacy Act Statement

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

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

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

Notice of Allowability	Application No. 16/603,252	Applicant(s) KOREN et al.	
	Examiner MOHAMMAD S SHAMS	Art Unit 2434	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 After final filed on 03/29/2021.
   ☐ 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 See Continuation Sheet . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

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

   Certified copies:

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

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

   * Certified copies not received: _____ .

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

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

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

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

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☑ Interview Summary (PTO-413), Paper No./Mail Date. 04/13/2021.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/MOHAMMAD S SHAMS/ Examiner, Art Unit 2434	/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498

Continuation of 3. The allowed claim(s) is/are: 1-5,7-9,12-15,17-20,24 and 26-28

DETAILED ACTION

1. Claims 1-5, 7-9, 12-15, 17-20, 24, and 26-28 are allowed.
2. This office action is in response after final filed on March 29, 2021. Claims 1, 4-5, 7, 12, 15, 17-18, and 24 have been amended. Claims 6, 10-11, 16, 21-23, and 25 have been canceled. No claims have been added. Therefore, claims 1-5, 7-9, 12-15, 17-20, 24, and 26-28 are presented here. Claims 1, 12, 24 are independent.

   The prior office actions incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

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.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the records appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.
   Authorization for this examiner's amendment was given in a telephone interview with attorney Caleb Pollack, Reg. No.37,912 on 04/13/2021.

The application has been amended as follows:

In the claims:

24. (Currently Amended) A system for dynamic management of private data during communication between a remote server and at least one user's device, the system comprising: a memory; a communication data type database, comprising at least one communication data type corresponding to sharing of at least one data packet from the user's device; a privacy preference database, comprising a list of allowed types of data packets for sharing during communication with the at least one user's device; a communication module, to allow communication between the remote server and the at least one user's device; and a processor, coupled to a response database and to the privacy preference database, wherein the processor is configured to instruct the remote server to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of data packets for sharing, and wherein the at least one data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device.

Allowable Subject Matter

4. Claims 1-5, 7-9, 12-15, 17-20, 24, and 26-28 are allowed over prior art of record.

Examiner's Statement of Reason for Allowance

5. The following is an examiner's statement of reason for allowance: Independent claims 1, 12, and 24 are allowed in view of prior art.

The closest prior art of Moffat et al. (US PGPUB No. 2013/0318347) discloses, a novel architecture for a data sharing system (DSS) is disclosed and seeks to ensure the privacy and security of users' personal information. In this type of network, a user's personally identifiable information is stored and transmitted in an encrypted form, with few exceptions. The only key with which that encrypted data can be decrypted, and thus viewed, remains in the sole possession of the user and the user's friends/contacts within the system. This arrangement ensures that a user's personally identifiable information cannot be examined by anyone other than the user or his friends/contacts. This arrangement also makes it more difficult for the web site or service hosting the DSS to exploit its users' personally identifiable information. Such a system facilitates the encryption, storage, exchange and decryption of personal, confidential and/or proprietary data.

The prior art of Vaha-Sipila et al. (US PGPUB No. 2012/0222081) discloses, an approach for maintaining user privacy information is described. A privacy management platform determines a request, from one or more applications, for access to local data associated with a device. The platform then determines and processes one or more privacy profile objects associated with the local data to determine one or more privacy policies associated with the local data, the device, or a combination thereof. Enforcement of the one or more privacy policies is then caused for granting access to the local data.

The prior art of Joseph et al. (US Patent No. 6,965,992) discloses, a method and system for network security includes a first network device having a first set of key material with a base key and a key extension, and a second network device also having the first set of key material and a second set of key material with a second base key. The second network device is capable of communicating with the first network device using security determined by the first set of key material. The method and system for network security may further include a third network device having the second set of key material. The third network device is capable of communicating with the second network device using security determined by the second set of key material. For the present method and system, security determined by the first set of key material is stronger than security determined by the second set of key material.

The prior art of Irvin et al. (US PGPUB No. 2010/0058054) discloses, this invention allows users to maximize their use of existing storage, processing power and network bandwidth resources. This is achieved through providing an enhanced level of data backup and restore that employs the initial encryption of data and storing one user's data on another user's hard drives through an anonymsing process. The efficiency of this process is enhanced when this invention is used in conjunction with self-authentication which then provides the ability to log into a network anonymously from potentially anywhere.

The prior art of Ling et al. (US PGPUB No. 2017/0041297) discloses, systems and methods are directed towards network data leakage prevention (DLP). More specifically, the systems and methods are directed towards using TCP

(Transmission Control Protocol) data packets in conjunction with the DLP monitor. The network DLP utilizes TCP data packets to carry source user identity. With the source user identity, the DLP monitor can determine if sensitive data can be transmitted based on the provided user information and corresponding DLP policies for each user. Furthermore, the DLP monitor can determine if sensitive data can also be transmitted for particular users in situations where multiple users share the same IP address.

The prior art of Gutt et al. (US PGPUB No. 2013/0305044) discloses, a system and method for verifying and/or geolocating network nodes in a network in attenuated environments for cyber and network security applications are disclosed. The system involves an origination network node, a destination network node, and at least one router network node. The origination network node is configured for transmitting a data packet downstream to the destination network node through at least one router network node. The data packet contains a header portion and a payload data portion. At least one of the network nodes is an enabled network node. The enabled network node(s) is configured to verify any of the network nodes that are located upstream from the enabled network node(s) by analyzing the header portion and/or the payload data portion of the data packet.

None of the prior art of record teaches or makes obvious the following limitation recited in independent claim 1 and similar limitations recited in independent claims 12 and 24 considering the claims as a whole: “A method of dynamic management of private data during communication between a remote server and a user's device, the method comprising: receiving, by the user's device, a request for retrieval of at least

one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request; determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device; receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication; modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference; and maintaining communication between the remote server and the user's device, with sharing of the modified data packets."

None of the prior arts of record either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed. Therefore, claims 1, 12, and 24 are considered to be allowable.

Dependent claims 2-5, 7-9, 13-15, 17-20, and 26-28 depend upon the above-mentioned allowable claims 1, 12, and are therefore allowed by virtue of their dependency.

6. Any comments Applicants considers necessary must be submitted no later than the payment of the Issue Fee and to avoid processing delays, should preferable accompany the Issue Fees. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance". In event of any post-allowance papers (e.g. IDS, 312 amendment, petition, etc.), Applicant is exhorted to mail papers to Production Control branch in Publications or faxed to post-allowance papers correspondence branch at (703) 308-5864 to expedite issuing process or call PUB's Customer Service if any questions at (703) 305-8497.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MOHAMMAD S SHAMS whose telephone number is (571)272-3406. The examiner can normally be reached on Monday-Friday 8:00 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. 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 https://ppair-my.uspto.gov/pair/PrivatePair. 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.

/MOHAMMAD S SHAMS/
Examiner, Art Unit 2434

/SAMSON B LEMMA/
Primary Examiner, Art Unit 2498

Examiner-Initiated Interview Summary	Application No. 16/603,252	Applicant(s) KOREN et al.		
	Examiner MOHAMMAD S SHAMS	Art Unit 2434	AIA (First Inventor to File) Status Yes	Page 1 of 1

All Participants (applicant, applicants representative, PTO personnel)	Title	Type
MOHAMMAD S SHAMS	Examiner	Telephonic
Samson Lemma	Primary Examiner	
Caleb Pollack, Reg. No. 37,912	Attorney of Record	

Date of Interview: 13 April 2021

Issues Discussed:

35 U.S.C. 101

On April 13th 2021 Applicant's representative Caleb Pollack Reg. No. 37,912 and Examiner together with the Primary examiner discussed and proposed examiner's amendment to place the application in better condition for allowance. Regarding independent claim 24 it has been proposed to include "a memory;" in the claim. Subsequently, on Sunday April 18th 2021 the proposed amendment has been accepted.

Proposed Amendment(s)

Please see the proposed examiner's amendment.

/MOHAMMAD S SHAMS/ Examiner, Art Unit 2434	/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498

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

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

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

Notice of References Cited	Application/Control No. 16/603,252	Applicant(s)/Patent Under Reexamination KOREN et al.	
	Examiner MOHAMMAD S SHAMS	Art Unit 2434	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-20170041297-A1	02-2017	Ling; Hui	H04L63/061	1/1
*	B	US-20100058054-A1	03-2010	IRVINE; David	H04L63/08	713/165
*	C	US-6965992-B1	11-2005	Joseph; Boby	H04L63/0428	380/281
*	D	US-20130305044-A1	11-2013	Gutt; Gregory M.	H04L63/1466	713/160
	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

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Management and Search of private data on Storage clouds Bernardo Ferreria, Henrique Domingos SDMCMM '12: Proceedings of the Workshop on Secure and Dependable Middleware for Cloud Monitoring and ManagementDecember 2012, Article No.: 4, pp 1–6 (Year: 2012)
	V	A survey of mobile cloud computing: architecture, applications, and approaches Hoang T. Dinh, Chonho Lee, Dusit Niyato, Ping Wang School of Computer Engineering, Nanyang Technological University (NTU) Singapore Published online Library pp. 1-25 (Year: 2011)
	W	Differentially Private Data Cubes: Optimizing Noise Sources and Consistency Bolin Ding, Marianne Winslett, Jiawei Han, Zhenhui Li SIGMOD '11: Proceedings of of the 2011 ACM SIGMOD International Conference on Management of data . June 2011, pp 217–228 (Year: 2011)
	X	

*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.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/603,252	KOREN et al.
	Examiner	Art Unit
	MOHAMMAD S SHAMS	2434

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

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

CLAIM		DATE								
Final	Original	09/19/2020	01/24/2021	04/06/2021						
	1	✓	✓	=						
	2	✓	✓	=						
	3	✓	✓	=						
	4	✓	✓	=						
	5	✓	✓	=						
	6	-	-	-						
	7	✓	✓	=						
	8	✓	✓	=						
	9	✓	✓	=						
	10	-	-	-						
	11	-	-	-						
	12	✓	✓	=						
	13	✓	✓	=						
	14	✓	✓	=						
	15	✓	✓	=						
	16	-	-	-						
	17	✓	✓	=						
	18	✓	✓	=						
	19	✓	✓	=						
	20	✓	✓	=						
	21	-	-	-						
	22	-	-	-						
	23	-	-	-						
	24	✓	✓	=						
	25	-	-	-						
	26	✓	✓	=						
	27	✓	✓	=						
	28	✓	✓	=						

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/603,252	KOREN et al.
	Examiner	Art Unit
	MOHAMMAD S SHAMS	2434

CPC						
Symbol					Type	Version
G06F	/	21	/	6263	F	2013-01-01
H04L	/	63	/	0421	I	2013-01-01
H04L	/	63	/	0428	I	2013-01-01

CPC Combination Sets								
Symbol					Type	Set	Ranking	Version
	/		/					

/MOHAMMAD S SHAMS/ Examiner, Art Unit 2434	05 April 2021	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498	08 April 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20210405

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/603,252	KOREN et al.
	Examiner	Art Unit
	MOHAMMAD S SHAMS	2434

INTERNATIONAL CLASSIFICATION					
CLAIMED					
G06F	/	21	/	62	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS

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

/MOHAMMAD S SHAMS/ Examiner, Art Unit 2434	05 April 2021	Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498	08 April 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20210405

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/603,252	KOREN et al.
	Examiner	Art Unit
	MOHAMMAD S SHAMS	2434

☐ 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	1	-	10	15	19	20	28								
2	2	-	11	16	20										
3	3	9	12	-	21										
4	4	10	13	-	22										
5	5	11	14	-	23										
-	6	12	15	17	24										
6	7	-	16	-	25										
7	8	13	17	18	26										
8	9	14	18	19	27										

/MOHAMMAD S SHAMS/ Examiner, Art Unit 2434	05 April 2021	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498	08 April 2021	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

U.S. Patent and Trademark Office — Part of Paper No.: 20210405

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/603,252	KOREN et al.
	Examiner	Art Unit
	MOHAMMAD S SHAMS	2434

CPC - Searched*		
Symbol	Date	Examiner
G06F21/6263, H04L63/0421, H04L63/0428	09/17/2020	M.S.S.

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
726	9	09/17/2020	

* 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
Applicant and Inventors Search	09/10/2020	M.S.S.
NPL, IP.com Search	09/17/2020	M.S.S.
EAST (Text and CPC) Search	09/22/2020	M.S.S.
Updated Applicant and Inventor(s) Search	01/23/2021	M.S.S.
Updated NPL, IP.com, and Google scholar search	01/23/2021	M.S.S.
Updated EAST (Text and CPC) Search	01/23/2021	M.S.S.
Updated Applicant and Inventor(s) Search	04/05/2021, 04/06/2021	M.S.S.
Updated NPL, IP.com, ACM DL and Google Scholar Search	04/05/2021	M.S.S.
Updated EAST (Text, CPC and interference) Search	04/06/2021	M.S.S.
Allowance have been approved by the SPE	04/03/2021	M.S.S.

/MOHAMMAD S SHAMS/ Examiner, Art Unit 2434	/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/603,252	KOREN et al.
	Examiner	Art Unit
	MOHAMMAD S SHAMS	2434

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**
G06F	21/6263	04/06/2021	M.S.S.
H04L	63/0421	04/06/2021	M.S.S.
H04L	63/0428	04/06/2021	M.S.S.

/MOHAMMAD S SHAMS/ Examiner, Art Unit 2434	/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498

Bibliographic Data

Application No: 16/603,252

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 AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/07/2019	726	2434	P-566702-US
RULE			

APPLICANTS

Privacy Rating Ltd., Ganey Tikva, ISRAEL

INVENTORS

Yoseph KOREN, Ganey Tikva, ISRAEL

Yehonatan WASSERMAN, Kiryat Ono, ISRAEL

CONTINUING DATA

This application is a 371 of PCT/IL2018/050359 03/28/2018

FOREIGN APPLICATIONS

ISRAEL IL251683 04/09/2017

IF REQUIRED, FOREIGN LICENSE GRANTED**

08/27/2020

**** SMALL ENTITY ****

STATE OR COUNTRY

ISRAEL

ADDRESS

Pearl Cohen Zedek Latzer Baratz LLP

7 Times Square, 19th Floor

New York, NY 10036

UNITED STATES

FILING FEE RECEIVED

$790

Context-awareness on mobile **devices**-the hydrogen **approach**

T Hofer, W Schwinger, M Pichler... - 36th annual Hawaii ..., 2003 - ieeexplore.ieee.org

... other approaches is that the three layers are located on one **device** thus making the **approach** robust against ... The call of the **method** doSomething() is linked to an event; by subscribing a listener to it the ... These **methods** are called, when an object is transmitted over a connection ...

☆ 99 Cited by 569 Related articles All 10 versions »

The personal **server**: Changing the **way** we think about ubiquitous computing

R Want, T Pering, G Danneels, M Kumar... - International Conference ..., 2002 - Springer

... central **server**, the system could use some kind of distributed file system **technique**, such as ... still continuing to operate, instead of just putting itself into a non-active sleep **mode** ... **Techniques** such as closed loop power monitoring, which allows the processor to actively monitor the ...

☆ 99 Cited by 360 Related articles All 23 versions »

A survey of mobile cloud computing: architecture, applications, and approaches

HT Dinh, C Lee, D Niyato... - Wireless **communications** ..., 2013 - Wiley Online Library

... Computation offloading **technique** is proposed **with** the objective to migrate the large computations and ... 18 and Smailagic and Ettus 19 evaluate the effectiveness of offloading **techniques** through several ... resources on a fine-grained, self-service basis is a flexible **way** for service ...

☆ 99 Cited by 2690 Related articles All 10 versions »

Gearing resource-poor mobile **devices with** powerful clouds: architectures, challenges, and applications

F Liu, P Shu, H Jin, L Ding, J Yu... - ... **communications**, 2013 - ieeexplore.ieee.org

... it takes a con- siderable amount of time for programmers to annotate offloadable **methods** ... However, this **approach** is mainly suitable for prefetch-friendly or delay-tolerant applications, such ... To address the problem, a **method** called “location cloaking” makes **user** location **data** ...

☆ 99 Cited by 401 Related articles All 8 versions

MyExperience: a system for *in situ* tracing and capturing of **user** feedback on mobile phones

J Froehlich, MY Chen, S Consolvo, B Harrison... - Proceedings of the 5th ..., 2007 - dl.acm.org

... Our **approach** is to combine both automatic tracing and **in** situ **user** experience sampling to ... Each Sensor descendant must override three **methods**: start the sensor, stop the sensor, and return ... components together from within the XML file and 2) it provides a **method** for injecting ...

☆ 99 Cited by 663 Related articles All 19 versions

Security and **privacy** challenges **in** mobile cloud computing: Survey and **way** ahead

MB Mollah, MAK Azad, A Vasilakos - Journal of Network and Computer ..., 2017 - Elsevier

... 2015), the mobile **users** can use the cloud services **in** easier **way** than past ... The computational offloading **technique** is introduced to overcome this kind of challenge ... However, virtualization **techniques** when applied to MCC, generates several security challenges (Sgandurra and ...

☆ 99 Cited by 178 Related articles All 7 versions

Quire: Lightweight provenance for smart **phone** operating systems

M Dietz, S Shekhar, Y Pisetsky, A Shu ... - USENIX security ..., 2011 - usenix.org

... This **approach** to permissions enables applications that have permission to access a resource to act as ... This leads us inevitably to **techniques** from the field of trusted platform measurement (TPM), where ... the process-id component to allow the recipient of an IPC **method** call to ...

☆ 99 Cited by 492 Related articles All 18 versions »

Thinkair: **Dynamic** resource allocation and parallel execution **in** the cloud for mobile code offloading

S Kosta, A Aucinas, P Hui, R Mortier... - 2012 Proceedings IEEE ..., 2012 - ieeexplore.ieee.org

... state, it takes on average 32s to start it, which is very high to use for **methods** that run ... Our **approach** for parallelization considers intervals of input values ... discount the affect of pre-emption by another process; • Number of instructions executed 5; • Number of **method** calls; • Thread ...

☆ 99 Cited by 1285 Related articles All 16 versions

Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing

K Gai, M Qiu, H Zhao, L Tao, Z Zong - Journal of Network and Computer ..., 2016 - Elsevier

... We develop a motivational example explaining the fundamental **methods** of adopting DECM ... This **approach** keeps the **communications in** the box containing the specific cloud **servers** and ... Figure 3 represents a conceptual work flow describing the **method** of DECM operations ...

☆ 99 Cited by 466 Related articles All 8 versions

Mobile wireless computing: Challenges **in data management**

T Imielinski, BR Badrinath - Communications of the ACM, 1994 - dl.acm.org

... The power requirement **in** "doze" **mode** is only 50uW ... Assuming this assump- tion is mostly valid, this locating **method** should be close to optimal ... Page 7. their calling (messaging) patterns, the overall performance of search and locating **methods** can be dramatically improved ...

☆ 99 Cited by 934 Related articles All 8 versions

"Ok to enter" /MSS/ 04/06/2021

Attorney Docket No.: P-566702-US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	KOREN, Yoseph et al.	Examiner:	Shams, Mohammad S
Serial No.:	16/603,252	Group Art Unit:	2434
Filed:	October 07, 2019	Confirmation No.:	6147
Title:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA		

RESPONSE

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

Sir/Madam:

This Response is being filed in response to the Final Office Action mailed January 29, 2021 by the United States Patent and Trademark Office in connection with the above-identified Application. A response to the January 29, 2021 Final Office Action is due April 29, 2021. Accordingly, this paper is being timely filed.

Remarks/Arguments begin on page **2** of this paper.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L13	1	"20120222083"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2021/04/06 09:50
L14	5	(("20090150968") or ("20100058054") or ("20100046749") or ("6965992") or ("20030163697")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/04/06 10:28
L15	62,264	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2021/04/06 10:29
L16	2	L14 and L15	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2021/04/06 10:29
L17	2	"20130305044"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2021/04/06 10:45
S1	0	((("PRIVACY") near3 ("RATING") near3 ("LTD"))).AS,AANM.	USPAT	OR	ON	2020/09/10 17:21
S2	1	((("KOREN") near3 ("Yoseph"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/10 17:21
S3	1	((("WASSERMAN") near3 ("Yehonatan"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/10 17:21
S4	2	dynamic near2 management near2 private near2 data	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/10 17:22
S6	58,795	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/10 17:28
S7	1	S2 and S6	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/10 17:35
S8	1	S6 and S3	US-PGPUB; USPAT;	OR	ON	2020/09/10 17:36

			USOCR; FPRS; EPO			
S9	28	(("20190347442") or ("20190182903") or ("20170325286") or ("10708978") or ("10212761") or ("20190342749") or ("10278065") or ("20180049023") or ("20170187758") or ("20100274859") or ("9781170") or ("20170230427") or ("20170230426") or ("10051018") or ("20190034060") or ("20190034826") or ("20190075140") or ("20160119330") or ("20190036775")).PN.	US-PGPUB; USPAT; USOCR; FPRS	OR	OFF	2020/09/12 16:34
S10	23	(("9954907") or ("20100064307") or ("20170041381") or ("10567479") or ("9197600") or ("10467552") or ("20140259147") or ("20180359811") or ("20040042414") or ("20090147772") or ("20170180504") or ("20190238655") or ("20160105416") or ("10306009") or ("8613026") or ("20170359420") or ("20120290844")).PN.	US-PGPUB; USPAT; USOCR; FPRS	OR	OFF	2020/09/12 16:45
S11	26	(("10402580") or ("8804966") or ("20090080661") or ("20190280986") or ("20170257143") or ("20190319932") or ("20180241727") or ("20150100488") or ("20180198757") or ("10491575") or ("10397335") or ("20200067884") or ("8254582") or ("20160219024")).PN.	US-PGPUB; USPAT; USOCR; FPRS	OR	OFF	2020/09/12 16:46
S12	77	S9 S10 S11	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/12 16:46
S15	2	"20130318347"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/12 16:59
S16	6	(("20090150968") or ("20070172066") or ("20100095119") or ("20040010467") or ("20100031335") or ("20100046749")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2020/09/12 17:08
S19	7	"2013318347"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2020/09/17 14:04
S20	2	"20130318347"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2020/09/17 14:04

S21	1	"20190149523"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/17 15:23
S22	10	"10348715"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/17 15:24
S23	6	"20170118638"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/17 15:28
S34	0	"16603252"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/18 09:31
S35	3	"10277614"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/18 10:27
S36	6	"20170118638"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/19 07:49
S37	3	"20150180839"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/19 07:50
S38	4	"20170054674"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/19 07:51
S39	2	"20160323305"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 11:04
S41	322,293	(request$3 ask$3 seek$3 requir$3 solicit$3) with (shar$3 exchang$3 communicat$3 exchang$3) and (compatiblity agreeable matched incompatible acceptable)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:36
S42	77	S41 and (privacy secrecy privateness confidentiality) near5 (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:37
S43	58,877	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT;	OR	ON	2020/09/21 15:38

			USOCR; FPRS; EPO			
S44	588	"L1" and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:38
S45	27	S42 and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:39
S46	4	"20020015422"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:09
S47	4	"20140119380"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:13
S48	44	S42 and ((characteristics traits identify$3 attributes pattern) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:19
S49	39	S41 and (privacy secrecy privateness confidentiality) near5 (data near2 packet) same (shar$3 exchang$3 communicat$3 exchang$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:48
S50	2	S49 and (modify$3 alter$3 revis$3 adjust$3 amend$3 modulat$3 chang$3) near5 (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:51
S51	12	S42 and ((modificat$3 chang$3 alter$3 revis$3 adjust$3 amend$3) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 21:21
S56	0	S41 and ((modificat$3 chang$3 alter$3 revis$3 adjust$3 amend$3) with (data near2 packet)) same ((incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 21:58
S57	0	S41 and (privacy secrecy privateness confidentiality) near5 (data near2 packet) same (incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:01
S58	0	S44 and (privacy secrecy privateness confidentiality) near5 (data near2	US-PGPUB; USPAT;	OR	ON	2020/09/21 22:01

		packet) same (incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security)	USOCR; FPRS; EPO			
S59	31	S44 and (incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:02
S60	3,093	S41 and (incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:10
S61	475	S60 and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:10
S62	6	S61 and (privacy secrecy privateness confidentiality) near5 (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:12
S63	3,911	((outgoing transmit$4 send$3) with (data packet information)) same (privacy near4 (set$4 policy rule))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:25
S64	468	((outgoing transmit$4 send$3) with (data packet information)) same (privacy near4 (set$4 policy rule)) with (complian$2 comply$3 complies violat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:27
S65	1,516	((outgoing transmit$4 send$3) with (data packet information)) same ((privacy security) near4 (set$4 policy rule)) with (complian$2 comply$3 complies violat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:28
S66	58,901	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:29
S67	88	S65 and S66	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:29
S68	5	S67 and ((modificat$3 chang$3 alter$3 revis$3 adjust$3 amend$3) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 13:54
S69	6	"20120005720"	US-PGPUB; USPAT;	OR	ON	2020/09/22 15:01

			USOCR; FPRS; EPO			
S71	2	"20130318347"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/19 12:46
S72	2	"20090150968"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/19 13:26
S73	5	"20180082058"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 11:45
S74	1	"20180276375"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 11:45
S75	2	"20130318347"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 11:53
S77	60,667	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2021/01/20 12:56
S78	6	(("20090150968") or ("20070172066") or ("20100095119") or ("20040010467") or ("20100031335") or ("20100046749")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/20 12:56
S79	0	S77 and S78	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 12:56
S80	16	(("20200387637") or ("20190347442") or ("10778730") or ("20170325286") or ("20190182903") or ("10708978") or ("10212761") or ("20190342749") or ("20180049023") or ("10278065") or ("10785641") or ("20100274859") or ("20170187758") or ("9781170") or ("20170230427") or ("20170230426")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/20 13:00
S81	15	(("20190034060") or ("20040042414") or ("20190034826") or ("20160308907") or ("10051018") or ("20190075140") or ("20190036775") or ("20030135587") or ("9954907") or ("20160119330") or ("9749293") or ("20140331054") or ("10467552") or ("20140259147") or ("20120290844")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/20 13:00

S82	16	(("9197600") or ("20090080661") or ("20040143738") or ("20200356618") or ("20170041381") or ("8804966") or ("10567479") or ("20090147772") or ("9660961") or ("20200084285") or ("8254582") or ("20170359420") or ("20170180504") or ("20200394246") or ("20190238655") or ("20160105416")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/20 13:00
S83	47	S80 S81 S82	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 13:01
S84	10	S83 and S77	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 13:01
S85	6	"20120005720"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 17:26
S86	32	"7676526"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 10:15
S87	4	"20140032228"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 10:40
S88	8	"20050066134"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 10:45
S92	4,644	(management governance monitor$3 plann$3) with (private encrpt$3 obfuscat$2) near2 data	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:09
S93	3,092	S92 and (server (remote near2 server) host) with (user client)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:11
S94	691	S93 and (read scanned allowed) with ((data near2 packet) file)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:17
S95	691	S92 and (server (remote near2 server) host) with (user client) and ((read scanned allowed) with ((data near2 packet) file))	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:18
S96	69	S95 and (G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:20
S97	3	S96 and (restricted modified controlled banned unread) with (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:30

S98	49	S96 and (restricted modified controlled banned unread) with data	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:32
S99	11	"9477836"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 18:17
S100	24	"9609025"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 19:29
S101	4	"20170098215"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 19:35
S103	22	S98 and (@ad<"20170409")	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 22:16
S104	17,199	(data near2 packet) with ("not read" restricted modified controlled banned unread)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/22 18:18
S105	67	S104 and (privacy secrecy privateness confidentiality) near5 (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/22 18:20
S106	20	S105 and (G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/22 18:20
S107	1	"20120222083"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/22 18:55
S108	16	(("20200387637") or ("20190347442") or ("10778730") or ("20170325286") or ("20190182903") or ("10708978") or ("10212761") or ("20190342749") or ("20180049023") or ("10278065") or ("10785641") or ("20100274859") or ("20170187758") or ("9781170") or ("20170230427") or ("20170230426")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/23 10:14
S109	15	(("20190034060") or ("10051018") or ("20040042414") or ("20160308907") or ("20190034826") or ("20190075140") or ("20190036775") or ("20030135587") or ("9954907") or ("20160119330") or ("9749293") or ("20140331054") or ("10467552") or ("20140259147") or ("20120290844")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/23 10:15
S110	17	(("9197600") or ("20090080661") or ("20200356618") or ("20040143738") or ("20170041381") or ("8804966") or	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/23 10:15

		("10567479") or ("20090147772") or ("9660961") or ("8254582") or ("20200084285") or ("20170359420") or ("20170180504") or ("20200394246") or ("20190238655") or ("20200358858") or ("20160105416")).PN.				
S111	48	S108 S109 S110	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 10:16
S112	10	S111 and (G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 10:16
S113	2	((("PRIVACY") near3 ("RATING") near3 ("LTD"))).AS,AANM.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:03
S114	7	((("KOREN") near3 ("Yoseph"))).INV.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:04
S115	7	((("WASSERMAN") near3 ("Yehonatan"))).INV.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:04
S116	736,618	(mask$3 obfuscat$3 conceal$3 disguis$3 hid$3 dissimulat$3 cover$3) with (data (data near2 packet) information)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:07
S117	60,694	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:09
S118	7,323	S116 and S117	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:10
S119	331,370	(request$3 ask$3 seek$3 requir$3 solicit$3) with (shar$3 exchang$3 communicat$3 exchang$3) and (compatiblity agreeable matched incompatible acceptable)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:10
S120	62,853	S116 and S119	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:11
S121	3,128	S120 and ((characteristics traits identify$3 attributes pattern) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:12
S122	12	S121 and (privacy secrecy privateness confidentiality) near5 (data near2 packet) same (shar$3 exchang$3 communicat$3 exchang$3)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:14

S123	10	S122 and S117	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:15
S124	736,618	(mask$3 obfuscat$3 conceal$3 disguis$3 hid$3 dissimulat$3 cover$3) with (data (data near2 packet) information)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/24 07:01
S125	331,370	(request$3 ask$3 seek$3 requir$3 solicit$3) with (shar$3 exchang$3 communicat$3 exchang$3) and (compatiblity agreeable matched incompatible acceptable)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/24 07:01
S126	62,853	S124 and S125	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/24 07:01
S127	3,128	S126 and ((characteristics traits identify$3 attributes pattern) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/24 07:01
S128	12	S127 and (privacy secrecy privateness confidentiality) near5 (data near2 packet) same (shar$3 exchang$3 communicat$3 exchang$3)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/24 07:01
S129	8	((("KOREN") near3 ("Yoseph"))).INV.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/04/05 22:32
S130	4	((("PRIVACY") near3 ("RATING") near3 ("LTD"))).AS,AANM.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2021/04/05 22:33
S131	8	((("WASSERMAN") near3 ("Yehonatan"))).INV.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/04/05 22:35
S132	62,232	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/04/05 22:35
S133	8	S129 and S132	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/04/05 22:35
S134	3	S130 and S132	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/04/05 22:36
S135	8	S131 and S132	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/04/05 22:36

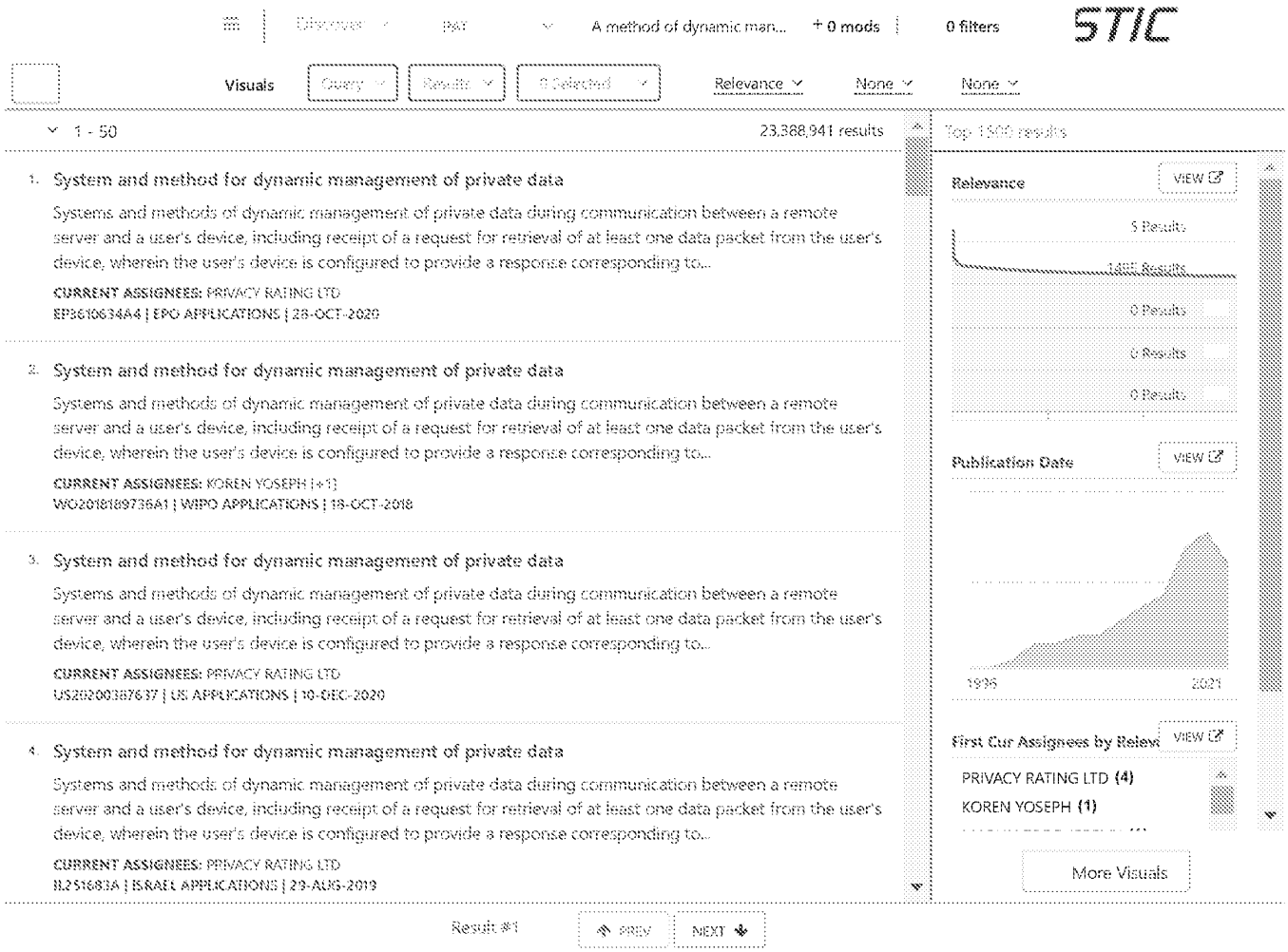
S136	336,909	(request$3 ask$3 seek$3 requir$3 solicit$3) with (shar$3 exchang$3 communicat$3 exchang$3) and (compatiblity agreeable matched incompatible acceptable)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/04/05 22:36
S137	12	((privacy secrecy privateness confidentiality) near5 (data near2 packet) same (shar$3 exchang$3 communicat$3 exchang$3)).CLM.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/04/05 22:38
S138	16	(("20200387637") or ("20190347442") or ("10778730") or ("20170325286") or ("20190182903") or ("10708978") or ("10212761") or ("20190342749") or ("10278065") or ("20180049023") or ("20210029535") or ("10785641") or ("20100274859") or ("20170187758") or ("9781170") or ("20170230427")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/04/05 22:41
S139	15	(("20170230426") or ("20190034060") or ("10051018") or ("20160308907") or ("20040042414") or ("20190034826") or ("20190075140") or ("20210067567") or ("20190036775") or ("20030135587") or ("9954907") or ("9749293") or ("20160119330") or ("20140331054") or ("10467552")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/04/05 22:41
S140	15	(("20140259147") or ("20120290844") or ("9197600") or ("20090080661") or ("20200356618") or ("20040143738") or ("20170041381") or ("8804966") or ("10567479") or ("9660961") or ("20090147772") or ("8254582") or ("20200084285") or ("20170359420") or ("20170180504")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/04/05 22:42
S141	11	(("20200394246") or ("10958745") or ("10306009") or ("20190238655") or ("20200358858") or ("20160105416") or ("10397335") or ("20170041401") or ("20210067577") or ("20090164470") or ("20190280986") or ("201703520864")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/04/05 22:42
S142	57	S138 S139 S140 S141	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/04/05 22:42
S143	11	S132 and S142	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/04/05 22:43

S144	0	(dynamic near2 management near2 private near2 data) and (request$3 ask$3 seek$3 requir$3 solicit$3) with (shar$3 exchang$3 communicat$3 exchang$3) and (compatiblity agreeable matched incompatible acceptable)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2021/04/05 23:41

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S145	5,239	((request$3 ask$3 seek$3 requir$3 solicit$3) with (shar$3 exchang$3 communicat$3 exchang$3) and (compatiblity agreeable matched incompatible acceptable)).CLM.	US-PGPUB; USPAT	OR	ON	2021/04/05 22:37
S146	13,566	(((characteristics traits identify$3 attributes pattern) with (data near2 packet))).CLM.	US-PGPUB; USPAT	OR	ON	2021/04/05 22:37
S147	12	((privacy secrecy privateness confidentiality) near5 (data near2 packet) same (shar$3 exchang$3 communicat$3 exchang$3)).CLM.	US-PGPUB; USPAT	OR	ON	2021/04/05 22:38
S148	28	S145 and S146	US-PGPUB; USPAT	OR	ON	2021/04/05 22:38
S149	28,798	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT	OR	ON	2021/04/05 22:38
S150	0	S148 and S147	US-PGPUB; USPAT	OR	ON	2021/04/05 22:39
S152	1	S147 and S149	US-PGPUB; USPAT	OR	ON	2021/04/05 22:40
S153	1	(((privacy secrecy privateness confidentiality) near5 (data near2 packet) same (shar$3 exchang$3 communicat$3 exchang$3)) and (dynamic near2 management near2 private near2 data)).CLM.	US-PGPUB; USPAT	OR	ON	2021/04/05 23:44

4/6/2021 1:40:36 PM
C:\Users\mshams\Documents\EAST\Workspaces\16603252.wsp


Discover
PAT
A method of dynamic man...
+ 0 mods
0 filters
STIC
Visuals
Query
Results
0 Selected
Relevance
None
None
1 - 50
23,388,941 results
Top 1500 results
1. System and method for dynamic management of private data
Systems and methods of dynamic management of private data during communication between a remote server and a user's device, including receipt of a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to...
CURRENT ASSIGNEES: PRIVACY RATING LTD
EP3610634A4 | EPO APPLICATIONS | 28-OCT-2020
2. System and method for dynamic management of private data
Systems and methods of dynamic management of private data during communication between a remote server and a user's device, including receipt of a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to...
CURRENT ASSIGNEES: KOREN YOSEPH [+1]
WO2018189736A1 | WIPO APPLICATIONS | 18-OCT-2018
3. System and method for dynamic management of private data
Systems and methods of dynamic management of private data during communication between a remote server and a user's device, including receipt of a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to...
CURRENT ASSIGNEES: PRIVACY RATING LTD
US20200387637 | US APPLICATIONS | 10-DEC-2020
4. System and method for dynamic management of private data
Systems and methods of dynamic management of private data during communication between a remote server and a user's device, including receipt of a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to...
CURRENT ASSIGNEES: PRIVACY RATING LTD
IL251683A | ISRAEL APPLICATIONS | 29-AUG-2019
Relevance
VIEW
5 Results
0 Results
0 Results
0 Results
Publication Date
VIEW
1996
2021
First Cur Assignees by Relev
VIEW
PRIVACY RATING LTD (4)
KOREN YOSEPH (1)
More Visuals
Result #1
PREV
NEXT

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
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 displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 16/603,252	Filing Date 10/07/2019	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ 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 $230 =	
☐ 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))					
* 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)			
AMENDMENT	03/29/2021	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $50 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $240 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)			
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 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ 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".	/VIOLA D ROGERS/
*** 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.

Attorney Docket No.: P-566702-US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	KOREN, Yoseph et al.	Examiner:	Shams, Mohammad S
Serial No.:	16/603,252	Group Art Unit:	2434
Filed:	October 07, 2019	Confirmation No.:	6147
Title:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA		

RESPONSE

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

Sir/Madam:

This Response is being filed in response to the Final Office Action mailed January 29, 2021 by the United States Patent and Trademark Office in connection with the above-identified Application. A response to the January 29, 2021 Final Office Action is due April 29, 2021. Accordingly, this paper is being timely filed.

Remarks/Arguments begin on page **2** of this paper.

REMARKS

The present response is intended to be fully responsive to all points of objection and/or rejection raised by the Examiner and is believed to place the application in condition for allowance.

Applicants assert that the present invention is new, non-obvious and useful. Prompt consideration and allowance of the claims is respectfully requested.

Status of Claims

Claims 1-5, 7-9, 12-15, 17-20, 24 and 26-28 are pending.

Claims 1-5, 7-9, 12-15, 17-20, 24 and 26-28 have been rejected.

CLAIM REJECTIONS

35 U.S.C. § 103 Rejections

In the Office Action, the Examiner rejected claims 1-5, 7-9, 12-15, 17-20, 24 and 26-28 under 35 U.S.C. § 103, as being unpatentable over Moffat (US Patent Publication No. 2013/0318347) in view of Vaha-Sipila et al. (US Patent Publication No. 2012/0222083).

Applicants respectfully traverse this rejection in view of the remarks that follow.

On pages 7-8 of the Final Office Action, the Examiner asserts Vahia-Sipla teaches determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device, as recited in independent claim 1. For these limitations the Examiner cites to Vaha-Siplia, para. [0070], and Fig. 5.

Applicants assert that Vaha-Sipila et al. is silent as to determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet, and wherein the content of

the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device, as recited at least in independent claim 1, and, therefore, cannot cure the deficiencies of Moffat.

According to paragraphs [0064] and [0070] of Vaha-Sipila et al., a privacy management platform determines a request for access to local data associated with a device, and determines one or more privacy profile objects associated with the local data, the device, or a combination thereof, where the privacy profile objects may be generated and made available for access by the privacy management platform by way of a third party and/or external policy provider, such as a non-governmental organization, open source data or software supplier or software task force that sets software policy standards and guidelines. Based on the determined privacy profile objects, the privacy management platform determines to perform various actions responsive to the determined object, where the local data includes, at least in part, sensor data associated with the device. Thus, Vaha-Sipila et al. describe the privacy management platform associating a privacy profile object with the local data.

Accordingly, Vaha-Sipila et al. cannot teach or suggest determining communication data type while the content is not read, for continued operation by the user's device in real time, since the data inspected by the privacy management platform is externally associated with a privacy profile. Therefore, when a new data packet is to be analyzed, the privacy management platform of Vaha-Sipila et al. cannot determine a communication data type since no privacy profile is associated with the new data packet and in order to analyze this new data, the content needs to be read until the new data is associated with a privacy profile.

In contrast, in the present independent claims the content of the at least one new data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device. For example, in the embodiment described in paragraph [062] of the present application, determination of data type does not read and concern (or take into consideration during the determination) the actual content of the data packet even if the content is encrypted.

Accordingly, Applicants respectfully assert that independent claim 1 is allowable over the above cited references. Similar arguments apply to independent claims 12 and 24, *mutatis mutandis*.

Each of claims 2-5, 7-9, 13-15, 17-20 and 26-28 depends, directly or indirectly, from one of independent claims 1, 12 and 24, and, therefore, includes all the limitations of the claim from which it depends. Therefore, Applicants respectfully assert that claims 2-5, 7-9, 13-15, 17-20 and 26-28 are likewise allowable.

Accordingly, Applicants respectfully request that the rejection of claims 1-5, 7-9, 12-15, 17-20, 24 and 26-28 under 35 U.S.C. § 103 be withdrawn.

Conclusion

In view of the foregoing remarks, Applicants assert that the pending claims are allowable. Their favorable reconsideration and allowance is respectfully requested.

Should the Examiner have any question or comment as to the form, content or entry of this paper, the Examiner is requested to contact the undersigned at the telephone number below. Similarly, if there are any further issues yet to be resolved to advance the prosecution of this application to issue, the Examiner is requested to telephone the undersigned counsel.

To the extent that there are any fees associated with this filing that are due but are not paid or are not able to be paid by a credit card mentioned elsewhere in this document, Applicants authorize the U.S. Patent and Trademark Office to charge any such fees to deposit account No. 60-2041.

Respectfully submitted,

/Caleb Pollack/

Caleb Pollack
Attorney/Agent for Applicant(s)
Registration No. 37,912

Dated: March 29, 2021

Pearl Cohen Zedek Latzer Baratz LLP
1500 Broadway, 12th Floor
New York, New York 10036
Tel: (646) 878-0800
Fax: (646) 878-0801

Electronic Acknowledgement Receipt

EFS ID:	42301753
Application Number:	16603252
International Application Number:	
Confirmation Number:	6147
Title of Invention:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA
First Named Inventor/Applicant Name:	Yoseph KOREN
Customer Number:	49443
Filer:	Caleb Pollack/Laura Saporta
Filer Authorized By:	Caleb Pollack
Attorney Docket Number:	P-566702-US
Receipt Date:	29-MAR-2021
Filing Date:	07-OCT-2019
Time Stamp:	06:52:49
Application Type:	U.S. National Stage under 35 USC 371

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		P-566702-US-RESFOA.pdf	31793 79261b9064e628551ec3750924788dc2ce5dfe5b	yes	4

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Response After Final Action	1	1
	Applicant Arguments/Remarks Made in an Amendment	2	4
Warnings:			
Information:			
	Total Files Size (in bytes):	31793	

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.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/603,252	10/07/2019	Yoseph KOREN	P-566702-US	6147

49443 7590 01/29/2021

Pearl Cohen Zedek Latzer Baratz LLP
7 Times Square, 19th Floor
New York, NY 10036

EXAMINER
SHAMS, MOHAMMAD S

ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
01/29/2021	ELECTRONIC

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

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

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

Arch-USPTO@PearlCohen.com
USPTO@PearlCohen.com

Office Action Summary	Application No. 16/603,252	Applicant(s) KOREN et al.	
	Examiner MOHAMMAD S SHAMS	Art Unit 2434	AIA (FITF) Status Yes

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

Period for Reply

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

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

Status

1)☑ Responsive to communication(s) filed on 12/27/2020.

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

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

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

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

Disposition of Claims*

5) ☑ Claim(s) 1-5,7-9,12-15,17-20,24 and 26-28 is/are pending in the application.

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

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-5,7-9,12-15,17-20,24 and 26-28 is/are rejected.

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

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

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

Application Papers

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

11)☑ The drawing(s) filed on 10/07/2019 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☑ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

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

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

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

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.

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

1. This office action is in response to amendment filed on December 27th, 20202. Claims 1, 4-5, 7, 12, 15, 17 and 24 have been amended. No new claims have been added. No claims have been canceled. Therefore, claims 1-5, 7-9, 12-15, 17-20, 24, and 26-28 are presented for examination.

   The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

Response to Arguments

2. Applicant's argument with respect to objection to amended claim is persuasive and thus the objection to claims 5 and 15 are withdrawn.

3. Applicant's argument with respect to rejection of claims 4, 7, 17-18, and 24 under 35 U.S.C. 112(b) is persuasive based on amended claims thus, the rejection under 112(b) is withdrawn.

4. Applicant's argument with respect to claim(s) 1, 12, and 24 have been considered but are moot because of the new ground of rejection does not rely on any reference applied in prior reference applied in prior rejection of record for any teachings or matter specifically challenged in the argument.

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.

The factual inquiries for establishing a background for determining obviousness under 35 U.S.C. 103 are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-5, 7-9, 12-15, 17-20, 24, and 26-28 are rejected under 35 U.S.C. 103 as being unpatentable over Moffat et al. (US PGPUB # 2013/0318347) in view of Vaha-Sipila et al. (US PGPUB # 2012/0222083).[This prior art is provided/cited in the IDS]

Regarding claim 1. Moffat does disclose, a method of dynamic management of private data during communication between a remote server and a user's device, the method comprising **[Moffat, para. 0232, FIG. 1, user's computing device 101 is connected to the Internet, or to some other electronic, digital or analog, data-sharing network…]**:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request **[Moffat, para. 0232, 0250, FIG. 1, FIG. 4, the DSS server receives data transmitted by the user's computer 101, and responds to requests for data by sending, when appropriate, messages and/or data back to the user's computer 101 via the Internet 103. (Para. 0250), FIG. 4 illustrates the actions and events which are typical of a user's interaction with the private DSS specified in an embodiment. User interaction begins 401 following the initialization of the DSS client on the user's computing device 101. Following initialization, the DSS client program (i.e. the "DSS_CP") operating on the user's computing device mediates 404 the user's interaction with the DSS server(s) by responding 404 to his interactions 402 with the DSS_CP, as well as responds 404 to messages, requests and data received 410 from the DSS server(s).]**;

~~determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device.~~

Moffat further discloses, receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication **[Moffat, para. 0149, 0221, 0826, the system of 6 wherein the unencrypted data includes permission-related attributes specifying what operations a recipient is allowed, by the owner, creator or source of the information specified by unencrypted data, to perform on that copy of the original information concealed within the encrypted data packet, including, but not limited to permissions regarding the recipient's printing, saving to local storage, editing, saving to external storage (e.g. a USB drive, a writable DVD, etc.), etc., of the copy of the original information. (Para. 0221) the DSS server will also determine the relevance of each packet of user data with respect to the type of media, e.g. the media-specific "page" or "section" of the "user interface" being viewed by a user on his local computing device by means of his DSS client. The relevance of each packet of user data might include not only the type of media, but also its date of creation and/or uploading, e.g. more recent media is often deemed to be more relevant to a user. The relevance of a packet of user data might also be affected by whether or not it is related to some other**

piece of user data, such as a comment on a photo. The relevance of any particular packet of user data might also be related to other attributes of that packet of data, as well as other attributes, characteristics, or user preferences, related to the context established by the DSS client and the other packets of user data to be displayed. (Para. 0826), the data can be represented and manipulated as explained below. Potentially sensitive and/or embarrassing user data is encrypted with an encryption key known only to the user who generates the data and only to the DSS client's of the recipients authorized by the user to receive, read, view, hear and/or otherwise experience that data. Therefore, original user data (such as text, photos and/or videos) is encrypted and only these encrypted forms of user data are stored and transmitted by the private DSS. Only in the DSS client program of an authorized user of the DSS, i.e. one possessing the requisite decryption key, can encrypted user data be restored and experienced.];

~~modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference~~; and

Moffat further discloses, maintaining communication between the remote server and the user's device, with sharing of the modified data packets **[Moffat, para. 0436, 0558, if the user who generated the requested data packet has opted to have the DSS server maintain a log of all processing associated with that packet (such as by the DSS server and/or by any other user's DSS client) then, in response to the request for the packet's retrieval, the DSS server can generate a log record that captures data about the packet's sharing (e.g. noting for example, the identity of the user who has directly, or indirectly, made the request and subsequently**

received the packet, the time and date of the request, and so forth). The DSS server 2207 then saves this log entry 2210 in its associated storage device(s) 2212 and subsequently (likely upon request by the user) provides that log entry (and any other log entries) to the user whose data has been manipulated and/or otherwise processed. (Para. 0804), Each of the client programs and/or program configurations that the server is capable of sending to a user can be capable of: performing a unique set of functions, the availability or lack thereof being detectable by the server (for example, responding to a specific query from the server); providing a unique set of responses to a set of queries from the server; and executing a unique set of modifications to data packets transmitted from the client to the server; etc.].

Moffat does not explicitly teach, determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device. and

modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference;

However Vaha-Sipila does teach determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received

request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device **[Vaha-Sipila, para. 0070, in FIG. 5, per steps 501-507 of process 500, the privacy management platform 103 determines to perform various actions responsive to the determined object. These may include determining to generate a prompt requesting an approval from a user of the device for the access, wherein the granting of the access is based, at least in part, on the approval (step 501); determining to generate an alert regarding the request (step 503); determining to apply at least one transformation to the local data, wherein the access is granted to the transformed local data (step 505); and causing, at least in part, denial of the access to at least a portion of the local data (step 507). It is noted that the local data includes, at least in part, sensor data associated with the device.]**; and

modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference **[Vaha-Sipila, para. 0035-0036 and 0061-0063, Table 3, Fig. 3-5 step 307, applying one or more transformations to the local data so that it is accessed in its transformed state, or denying access to the local data or a portion thereof. [0035] The transformation applied to the local data by system 100 may be executed by way of one or more equations or transformation rules, such that the means of presentment of data or acquisition of data is affected. By way of example, the data may be transformed such data is presented according to granularity level for the data, i.e., as based on at least one privacy**

policy[0035-0036]. (Para. 0061-0063), according to table 3, when the media and the location are shared, no change is applied to the media data and the location data, whereas the event data is changed before being shared based on a filter function defined for the user or application/service requesting the data. The personal data in this example is blocked from sharing. For a customer care, the media data and the location data may be accessed without any change, but the event data is blocked and the personal data is filtered. Also, for advertising, the media data may be accessed without any change, but the event data and the location data are blocked from the advertising service, and the personal data is filtered. Further, as discussed above, the transformation function may enforce both the primary usage and the sensitivity by enforcing a combination of table 3 and table 2 (e.g., table 3 [circle around (x)] table 2).].

Moffat and Vaha-Sipila are in the same field of endeavor as they both are pertaining to means to management and protecting user privacy information.

Therefore, it would have been obvious to one of ordinary skill in the art before the effective date of claimed invention to modify the teachings of Moffat that relates to a data sharing system (DSS) is disclosed and seeks to ensure the privacy and security of users' personal information (Moffat, please abstract and para. 0031) with the teachings of Vaha-Sipila (Vaha-Sipila, para. 0035-0036, and 0061-0063, 0070, FIG. 3-5, and table 3) would enable Moffat with a means to changing/ filtering any information or data that user may exchange with the a server through a privacy policy objective in order to protect the user's private information via a communication network.

Regarding claim 2. The combination of Moffat and Vaha-Sipila discloses the method of claim 1 above. Furthermore Moffat discloses, wherein the communication data type of the at least one data packet is determined from metadata of communication with the remote server **[Moffat, para. 0499, 0501, additional metadata would also be generated by the DSS, and stored locally on a user's computer by the DSS client, and/or stored within the DSS server. This metadata would be designed to provide the DSS with hints as to which other encrypted media elements are likely to be most relevant to a user's DSS client, with respect to any particular state of that DSS client. Some, or all, of such user data metadata might be encrypted and hidden from the DSS server if it would be deemed likely to contain user-related data, or if it might provide a risk to the security and/or privacy of user data. (Para. 0501), The generation and storage of such general and/or context-specific user data metadata can be particularly useful for embodiments in which only a minimal amount of information about the attributes of individual user data media elements is made available to the DSS server. When only a minimal amount of metadata, if any, is available to the DSS server to assist it in characterizing, sorting and prioritizing user data prior to its transmission to a DSS client, then metadata (especially metadata containing information related to relevance and priority of the media specified within the user data) would likely greatly improve the efficiency of future retrievals and/or transmissions of user data in response to requests by DSS clients.]**.

Regarding claim 3. The combination of Moffat and Vaha-Sipila discloses the method of claim 1 above. Furthermore Moffat discloses, the method/system further comprising:

determining, by the user's device, at least one communication data pattern of at least one data packet corresponding to the received request **[Moffat, para. 0611, heuristics based on attributes of each user's encrypted content, patterns of communication, network of contacts, and/or other factors discernable even in the absence of access to decrypted versions of the user data, will be used to identify those users most likely to be engaging in improper activities and/or to be storing and/or disseminating improper content; with the likelihood of random sampling of user data being at least partially influenced by the results of such analyses.]**; and

Moffat does not explicitly disclose, modifying data packets corresponding to requests for sharing of responses corresponding to at least one data pattern, that are not compatible with the received privacy preference, wherein the privacy preference comprises a list of allowed data patterns for sharing during communication.

However, Vaha-Sipila does teach, modifying data packets corresponding to requests for sharing of responses corresponding to at least one data pattern, that are not compatible with the received privacy preference, wherein the privacy preference comprises a list of allowed data patterns for sharing during communication **[Vaha-Sipila, et al. para. 0061-0063, Table 3, Fig. 3-5 step 307, according to table 3, when the media and the location are shared, no change is applied to the media data and the location data, <u>whereas the event data is changed before being shared based on a filter function defined for the user or application/service requesting the data</u>.**

The personal data in this example is blocked from sharing. For a customer care, the media data and the location data may be accessed without any change, but the event data is blocked and the personal data is filtered. Also, for advertising, the media data may be accessed without any change, but the event data and the location data are blocked from the advertising service, and the personal data is filtered. Further, as discussed above, the transformation function may enforce both the primary usage and the sensitivity by enforcing a combination of table 3 and table 2 (e.g., table 3 [circle around (x)] table 2).].

Moffat and Vaha-Sipila are in the same field of endeavor as they both are pertaining to means to management and protecting user privacy information.

Therefore, it would have been obvious to one of ordinary skill in the art before the effective date of claimed invention to modify the teachings of Moffat that relates to a data sharing system (DSS) is disclosed and seeks to ensure the privacy and security of users' personal information (Moffat, please abstract and para. 0031) with the teachings of Vaha-Sipila (Vaha-Sipila, para. 0061-0063, FIG. 3-5, and table 3) would enable Moffat with a means to changing/ filtering any information or data that user may exchange with the a server through a privacy policy objective in order to protect the user's private information via a communication network.

Regarding claim 4. The combination of Moffat and Vaha-Sipila discloses the method of claim 3 above. Furthermore Moffat discloses, wherein the communication data pattern is determined based on a range selected from a group consisting of data packet frequency, data packet size, data packet speed, data packet count, data packet

ratio compared to other data type flow, data packet repetition, and data packet order **[Moffat, para. 0122, The network of 1f in which some aspect of the sharing, including, but not limited to: the selection of data, products and/or services, the categories data, products and/or services, the quality data, products and/or services, the quantity of data, products and/or services, and/or the frequency of provision of data, products and/or services, may vary between a first and second other user. (Para. 0143), the system of 6 wherein the unencrypted data includes size of information specified by unencrypted data, e.g. original file size. (Para. 269), FIG. 7 is a simplified illustration of a basic data flow in a private DSS implemented in accordance with an embodiment herein. (Para. 0331), any attempt by the user 1301 to transmit a digital copy 1318 of the locally-stored copy of the document 1306 by means of some data distribution network 1319 (e.g. the Internet) to which his computing device 1302 is connected, to the computing device 1320 of some unauthorized recipient 1321, will only transmit the encrypted version of the document. (Para. 0334), the use of a private DSS of a type disclosed herein to control access to sensitive data within an organization benefits such organizations by making the copying and dissemination of sensitive data more difficult to perpetrate, more likely to be detected by others, more time-consuming and less likely to succeed.]**.

Regarding claim 5. The combination of Moffat and Vaha-Sipila discloses the method of claim 1 above. Furthermore Moffat discloses, wherein the communication data type is determined based on data packet characteristics selected from a group

consisting of data packet header, data packet footer, version number, IP (Internet Protocol) address, HTTPS (HyperText Transfer Protocol Secure), file extension, encryption method, encoding method, keywords, driver, and communication protocol **[Moffat, para. 0425, 0612, 0622, another optional safeguard which may help to ensure the integrity of the log-in process is for a private DSS to require that the entire DSS client always be uploaded to a user's computing device, immediately following a successful log in, by means of an encrypted (e.g. an https) connection. (Para. 0612), if one user tends to disseminate relatively large numbers of images to his contacts, while not receiving many messages, or other types of media, in return, that might increase the likelihood of improper conduct. They might be based on the distribution of types of media in a user's account. For instance, if a user stores large numbers of images and videos, but very few status messages, then that might be suggestive of someone storing improper content. Many other potential heuristics are possible, and the uses of all such heuristics for the purpose of identifying abusive users are included within the scope of the possible embodiments. (Para. 0622), the efficiency with which they monetize their private DSS by targeting ads to users on the basis of the geographical location of the user. The DSS client and/or DSS server should be able to identify the approximate location of a user based on the IP address from which the client connects to the corresponding data-sharing network, browser attributes and/or other available attributes.]**.

Regarding claim 7. The combination of Moffat and Vaha-Sipila discloses the method of claim 1 above. Furthermore Moffat discloses, further comprising:

determining, by the remote server, a communication data pattern of the at least one data packet of the received request **[Moffat, para. 0275, The DSS client responds to any new requests by the user for access to contact data by requesting any available encrypted contact data from the DSS server. Upon receipt of that encrypted contact data, the DSS server uses the contact's decryption key (stored in the user's key locker) to decrypt the data. When contacts of the user create, upload and/or modify any of their data, the DSS server passes that encrypted user data to the user's DSS client. And, again, the DSS client retrieves the needed decryption key(s) from the user's key locker and decrypts the encrypted contact data.]**; and

linking at least one response from the user's device to a type of data packet from the user's device, wherein the linking is based on the communication data type and communication data pattern of the at least one response **[Moffat, para. 0341, FIG. 14B illustrates a method by which a DSS_CP can be loaded directly on to a user's computing device 1402. A browser program 1410 running on a user's computing device 1402 can connect to a DSS server 1409, through a data distribution network 1411 like the Internet, if the user enters the proper URL into the appropriate browser input. The DSS server can then return an installer program, or a link to such an installer program, which the user can choose to download. After the installer 1412 is downloaded, the user can execute that installer resulting in the installation of a "stand-alone" DSS_CP 1413 capable of running**

without a browser on the user's computing device 1402. Such a stand-alone DSS_CP can likely incorporate more functionality than a typical browser-based program and it can likely facilitate a user's utilization of a private DSS which used an uncommon, or poorly supported, data distribution network, e.g., a proprietary network based on the transmission and distribution of data through the electrical wiring of a house or other building.].

Regarding claim 8. The combination of Moffat and Vaha-Sipila discloses the method of claim 1 above. Furthermore Moffat discloses, further comprising:

identifying a response corresponding to a request for sharing of data packets, wherein the identified response is not compatible with the received privacy preference **[Moffat, para. 0257, 0609, FIG. 5, the request will typically be transmitted through the data sharing network 504, e.g. the Internet, by the network I/O subsystem 506 of the user's computing device 505. (Para. 0609), utilize tools within the DSS client to look for and detect improper content. This would eliminate the need for compromising the privacy of any user's data until, and unless, content which appears to be abusive is detected.]**; and

providing a response with at least one modified data packet corresponding to the request for sharing types of data packets **[Moffat, para. 0826, the data can be represented and manipulated as explained below. Potentially sensitive and/or embarrassing user data is encrypted with an encryption key known only to the user who generates the data and only to the DSS client's of the recipients authorized by the user to receive, read, view, hear and/or otherwise experience**

that data. Therefore, original user data (such as text, photos and/or videos) is encrypted and only these encrypted forms of user data are stored and transmitted by the private DSS. Only in the DSS client program of an authorized user of the DSS, i.e. one possessing the requisite decryption key, can encrypted user data be restored and experienced.].

Regarding claim 9. The combination of Moffat and Vaha-Sipila discloses the method of claim 8 above. Furthermore Moffat discloses, wherein the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption **[Moffat, para. 0559-0561, 0826. users are offered the ability to create and modify repositories of data dedicated to the maintenance of "to-do lists," accounting data (both personal and business), and other types of archives dedicated to special purposes, and/or special types of data, in which the user is able to vary the data through additions, deletions, edits and so forth. (Para. 0560), users are able to elect to have all, or some select portion, of the information which they generate or discover online automatically copied to one or more special-purpose personal archives. In an embodiment, these archives can be edited, and otherwise manipulated. This allows a user the ability to construct a variety of collections of information gathered, and/or in some other way generated, through online activity of some kind. (Para. 0561), for instance, a user searching for online tools which facilitate a user's creation of graphical**

illustrations might elect to collect those tools, or annotated links to the locations where such tools can be found, as well as samples of artwork which the user has created with the tools evaluated. The user might, at some point, elect to reorganize, and fully document, this collection so that it will be suitable for sharing with others. (Para. 826), certain information will be made available to the DSS server regarding the various individual elements of user data. For example, in an embodiment, the DSS server stores and has access to the following information regarding each individual packet of data owned, authored, uploaded and/or associated with any particular user: (a) An identifier which uniquely identifies and distinguishes each data packet within the computers, servers and/or programs of the DSS server. (b) The media or data type, or category, of each data packet, e.g. original text, a comment on other media, photo, video, link, etc. (c) The relationship of each packet of data to any other packet(s) of data (if any), such as a comment related to some other piece of media. (d) The date and time at which each data packet, and/or the associated media stored therein, was created, uploaded, modified, etc. (Para. 0558), users are offered a number of "dynamic personal archives" as well as the "static," "write-once" archives discussed earlier. These dynamic personal archives allow users to create collections of data in which they can modify the contents over time through deletions, edits, etc. These dynamic archives can be implemented such that the frequent modification of the contents is facilitated.].

Regarding claim 12. Moffat does teach, a method of dynamic management of private data during communication between a remote server and a user's device, the method comprising **[Moffat, para. 0232, FIG. 1, user's computing device 101 is connected to the Internet, or to some other electronic, digital or analog, data-sharing network…]**:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request **[Moffat, para. 0232, 0250, FIG. 1, FIG. 4, the DSS server receives data transmitted by the user's computer 101, and responds to requests for data by sending, when appropriate, messages and/or data back to the user's computer 101 via the Internet 103. (Para. 0250), FIG. 4 illustrates the actions and events which are typical of a user's interaction with the private DSS specified in an embodiment. User interaction begins 401 following the initialization of the DSS client on the user's computing device 101. Following initialization, the DSS client program (i.e. the "DSS_CP") operating on the user's computing device mediates 404 the user's interaction with the DSS server(s) by responding 404 to his interactions 402 with the DSS_CP, as well as responds 404 to messages, requests and data received 410 from the DSS server(s).]**;

~~determining, by the remote server, at least one communication data pattern corresponding to the received request, wherein the at least one communication data pattern is determined in accordance with a behavior range of the communication data packet, and wherein the content of the at least one data packet is not read by the~~

~~remote server for continued operation by the user's device in real-time during communication between the remote server and the user's device.~~

Moffat further discloses, receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data patterns for sharing during communication **[Moffat, para. 0149, 0221, 0826, the system of 6 wherein the unencrypted data includes permission-related attributes specifying what operations a recipient is allowed, by the owner, creator or source of the information specified by unencrypted data, to perform on that copy of the original information concealed within the encrypted data packet, including, but not limited to permissions regarding the recipient's printing, saving to local storage, editing, saving to external storage (e.g. a USB drive, a writable DVD, etc.), etc., of the copy of the original information. (Para. 0221) the DSS server will also determine the relevance of each packet of user data with respect to the type of media, e.g. the media-specific "page" or "section" of the "user interface" being viewed by a user on his local computing device by means of his DSS client. The relevance of each packet of user data might include not only the type of media, but also its date of creation and/or uploading, e.g. more recent media is often deemed to be more relevant to a user. The relevance of a packet of user data might also be affected by whether or not it is related to some other piece of user data, such as a comment on a photo. The relevance of any particular packet of user data might also be related to other attributes of that packet of data, as well as other attributes, characteristics, or user preferences, related to the context established by the DSS client and the other packets of user data to be displayed.**

(Para. 0826), the data can be represented and manipulated as explained below. Potentially sensitive and/or embarrassing user data is encrypted with an encryption key known only to the user who generates the data and only to the DSS client's of the recipients authorized by the user to receive, read, view, hear and/or otherwise experience that data. Therefore, original user data (such as text, photos and/or videos) is encrypted and only these encrypted forms of user data are stored and transmitted by the private DSS. Only in the DSS client program of an authorized user of the DSS, i.e. one possessing the requisite decryption key, can encrypted user data be restored and experienced];

~~modifying data packets corresponding to requests for sharing of responses and corresponding data patterns that are not compatible with the received privacy preference;~~ and

Moffat further disclose, maintaining communication between the remote server and the user's device, with sharing of the modified data packets **[Moffat, para. 0436, 0558, if the user who generated the requested data packet has opted to have the DSS server maintain a log of all processing associated with that packet (such as by the DSS server and/or by any other user's DSS client) then, in response to the request for the packet's retrieval, the DSS server can generate a log record that captures data about the packet's sharing (e.g. noting for example, the identity of the user who has directly, or indirectly, made the request and subsequently received the packet, the time and date of the request, and so forth). The DSS server 2207 then saves this log entry 2210 in its associated storage device(s) 2212 and subsequently (likely upon request by the user) provides that log entry**

(and any other log entries) to the user whose data has been manipulated and/or otherwise processed. (Para. 0804), Each of the client programs and/or program configurations that the server is capable of sending to a user can be capable of: performing a unique set of functions, the availability or lack thereof being detectable by the server (for example, responding to a specific query from the server); providing a unique set of responses to a set of queries from the server; and executing a unique set of modifications to data packets transmitted from the client to the server; etc.].

Moffat does not explicitly teach, determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device. and

modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference.

However, Vaha-Sipila does teach, determining, by the remote server, at least one communication data pattern corresponding to the received request, wherein the at least one communication data pattern is determined in accordance with a behavior range of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's

device in real time during communication between the remote server and the user's device **[Vaha-Sipha, para. 0070, in FIG. 5, per steps 501-507 of process 500, the privacy management platform 103 determines to perform various actions responsive to the determined object. These may include determining to generate a prompt requesting an approval from a user of the device for the access, wherein the granting of the access is based, at least in part, on the approval (step 501); determining to generate an alert regarding the request (step 503); determining to apply at least one transformation to the local data, wherein the access is granted to the transformed local data (step 505); and causing, at least in part, denial of the access to at least a portion of the local data (step 507). It is noted that the local data includes, at least in part, sensor data associated with the device.]**; and

modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference **[Vaha-Sipila, Para. 0035-0036, and 0061-0063, Table 3, Fig. 3-5 step 307, applying one or more transformations to the local data so that it is accessed in its transformed state, or denying access to the local data or a portion thereof. [0035] The transformation applied to the local data by system 100 may be executed by way of one or more equations or transformation rules, such that the means of presentment of data or acquisition of data is affected. By way of example, the data may be transformed such data is presented according to granularity level for the data, i.e., as based on at least one privacy policy [0036]. (Para. 0061-0063), according to table 3, when the media and the location are shared, no change is applied to the media data and the location**

data, whereas the event data is changed before being shared based on a filter function defined for the user or application/service requesting the data. The personal data in this example is blocked from sharing. For a customer care, the media data and the location data may be accessed without any change, but the event data is blocked and the personal data is filtered. Also, for advertising, the media data may be accessed without any change, but the event data and the location data are blocked from the advertising service, and the personal data is filtered. Further, as discussed above, the transformation function may enforce both the primary usage and the sensitivity by enforcing a combination of table 3 and table 2 (e.g., table 3 [circle around (x)] table 2).].

Moffat and Vaha-Sipila are in the same field of endeavor as they both are pertaining to means to management and protecting user privacy information.

Therefore, it would have been obvious to one of ordinary skill in the art before the effective date of claimed invention to modify the teachings of Moffat that relates to a data sharing system (DSS) is disclosed and seeks to ensure the privacy and security of users' personal information (Moffat, please abstract and para. 0031) with the teachings of Vaha-Sipila (Vaha-Sipila, para. 0035-0036 and 0061-0063, 0070, FIG. 3-5, and table 3) would enable Moffat with a means to changing/ filtering any information or data that user may exchange with the a server through a privacy policy objective in order to protect the user's private information via a communication network.

Regarding claim 13. The combination of Moffat and Vaha-Sipila discloses the method of claim 12 above. Furthermore Moffat discloses, wherein the communication

data pattern of the at least one response is determined from metadata of communication with the remote server **[Moffat, para. 0499, 0501, additional metadata would also be generated by the DSS, and stored locally on a user's computer by the DSS client, and/or stored within the DSS server. This metadata would be designed to provide the DSS with hints as to which other encrypted media elements are likely to be most relevant to a user's DSS client, with respect to any particular state of that DSS client. Some, or all, of such user data metadata might be encrypted and hidden from the DSS server if it would be deemed likely to contain user-related data, or if it might provide a risk to the security and/or privacy of user data. (Para. 0501), The generation and storage of such general and/or context-specific user data metadata can be particularly useful for embodiments in which only a minimal amount of information about the attributes of individual user data media elements is made available to the DSS server. When only a minimal amount of metadata, if any, is available to the DSS server to assist it in characterizing, sorting and prioritizing user data prior to its transmission to a DSS client, then metadata (especially metadata containing information related to relevance and priority of the media specified within the user data) would likely greatly improve the efficiency of future retrievals and/or transmissions of user data in response to requests by DSS clients.]**.

Regarding claim 14. The combination of Moffat and Vaha-Sipila discloses the method of claim 12 above. Furthermore Moffat discloses, further comprising:

determining, by the remote server, the communication data type of the at least one data packet of the received request **[Moffat, para. certain information will be made available to the DSS server regarding the various individual elements of user data. For example, in an embodiment, the DSS server stores and has access to the following information regarding each individual packet of data owned, authored, uploaded and/or associated with any particular user: (a) An identifier which uniquely identifies and distinguishes each data packet within the computers, servers and/or programs of the DSS server. (b) The media or data type, or category, of each data packet, e.g. original text, a comment on other media, photo, video, link, etc. (c) The relationship of each packet of data to any other packet(s) of data (if any), such as a comment related to some other piece of media. (d) The date and time at which each data packet, and/or the associated media stored therein, was created, uploaded, modified, etc.]**; and

modifying data packets corresponding to requests for sharing of responses and corresponding data patterns **[Moffat, para. 0274, After this process of initialization, the DSS client begins a cyclic pattern of interaction with the DSS server. The DSS client requests 711 from the DSS server 712 any encrypted data from the user and/or contacts appropriate to the context of the DSS client's user interface. Upon receipt of the encrypted user data 715, the DSS client uses the appropriate decryption key(s) to decrypt that data 716. The DSS client, for example, then makes this decrypted user data available to the user via the user interface.]**,

~~corresponding to at least one communication data packet type, that are not compatible with the received privacy preference~~,

Moffat further discloses, wherein the privacy preference comprises a list of allowed data packet types for sharing during communication **[Moffat, para. 0149, 0221, 0826, the system of 6 wherein the unencrypted data includes permission-related attributes specifying what operations a recipient is allowed, by the owner, creator or source of the information specified by unencrypted data, to perform on that copy of the original information concealed within the encrypted data packet, including, but not limited to permissions regarding the recipient's printing, saving to local storage, editing, saving to external storage (e.g. a USB drive, a writable DVD, etc.), etc., of the copy of the original information. (Para. 0221) the DSS server will also determine the relevance of each packet of user data with respect to the type of media, e.g. the media-specific "page" or "section" of the "user interface" being viewed by a user on his local computing device by means of his DSS client. The relevance of each packet of user data might include not only the type of media, but also its date of creation and/or uploading, e.g. more recent media is often deemed to be more relevant to a user. The relevance of a packet of user data might also be affected by whether or not it is related to some other piece of user data, such as a comment on a photo. The relevance of any particular packet of user data might also be related to other attributes of that packet of data, as well as other attributes, characteristics, or user preferences, related to the context established by the DSS client and the other packets of user data to be displayed. (Para. 0826), the data can be represented and manipulated as explained below. Potentially sensitive and/or embarrassing user data is encrypted with an encryption key known only to the user who generates the data**

and only to the DSS client's of the recipients authorized by the user to receive, read, view, hear and/or otherwise experience that data. Therefore, original user data (such as text, photos and/or videos) is encrypted and only these encrypted forms of user data are stored and transmitted by the private DSS. Only in the DSS client program of an authorized user of the DSS, i.e. one possessing the requisite decryption key, can encrypted user data be restored and experienced.].

Moffat does not disclose, corresponding to at least one communication data packet type, that are not compatible with the received privacy preference,

However, Vaha-Sipila does disclose, corresponding to at least one communication data packet type, that are not compatible with the received privacy preference **[Vaha-Sipila, para. 0035, FIG. 1, in certain embodiments, objects are downloaded and installed to the user device by the privacy management platform 10. Responsive to processing or execution of the one or more privacy profile objects, the device is caused to enforce one or more privacy policies for granting the requesting application access to the local data. The system 100 enables various enforcement mechanisms to be employed, based at least in part on the particular object, policy to be enforced, and other factors. This may include causing presentation of an indicator to the user interface, the indicator being representative of the privacy policy object, generating a prompt requesting an approval from a user of the device for a granting of access to the local data, generating an alert regarding the request, applying one or more transformations**

to the local data so that it is accessed in its transformed state, or denying access to the local data or a portion thereof..].

Moffat and Vaha-Sipila are in the same field of endeavor as they both are pertaining to means to management and protecting user privacy information.

Therefore, it would have been obvious to one of ordinary skill in the art before the effective date of claimed invention to modify the teachings of Moffat that relates to a data sharing system (DSS) is disclosed and seeks to ensure the privacy and security of users' personal information (Moffat, please abstract and para. 0031) with the teachings of Vaha-Sipila (Vaha-Sipila, para. 0035, FIG. 1) would enable Moffat with a means to changing/ filtering any information or data that user may exchange with the a server through a privacy policy objective in order to protect the user's private information via a communication network.

Regarding method claim 15 that is same or similar to method claim 5, and is similarly rejected.

Regarding claim 17. The combination of Moffat and Vaha-Sipila discloses the method of claim 12 above. Furthermore Moffat discloses, wherein the user's device is in communication with an external database with at least one communication data pattern corresponding to a request for sharing of data packets from the user's device, and wherein at least one data pattern compatible with the received request is determined from the database **[Moffat, para. 0257, FIG. 5, The request will typically be transmitted through the data sharing network 504, e.g. the Internet, by the network I/O subsystem 506 of the user's computing device 505. After receiving**

the request for user data from the DSS_CP 509, the DSS system retrieves the user's encrypted data from storage 501, including but not limited to the user's encrypted key locker 502. And, after retrieving the encrypted key locker, the DSS system sends that encrypted file to the DSS_CP by means of the data sharing network 504.].

Regarding method claim 18 that is same or similar to method claim 7, and is similarly rejected.

Regarding method claim 19 that is same or similar to method claim 8, and is similarly rejected.

Regarding method claim 20 that is same or similar to method claim 9, and is similarly rejected.

Regarding claim 24. Moffat does teach, a system for dynamic management of private data during communication between a remote server and at least one user's device, the system comprising **[Moffat, para. 0232, FIG. 1, user's computing device 101 is connected to the Internet, or to some other electronic, digital or analog, data-sharing network…]:**

a communication data type database, comprising at least one communication data type corresponding to sharing of at least one data packet from the user's device **[Moffat, para. 0235, FIG. 2 illustrates a possible structure of a private DSS of a type of this disclosure. A group of users 201, 202, 203 creates accounts within the DSS 213. These users interact with the DSS 213 through local DSS client**

programs ("DSS_CP's") 205, 206, 207 running on their respective computing devices 208, 209, 210. These DSS_CP's utilize the hardware and software resources of the users' computing devices 208, 209, 210 to communicate with, and exchange data with, the DSS server(s) 204. The DSS_CP's 205, 206, 207 only transmit encrypted versions of any user data transmitted into the Internet or other data sharing network 211. And, only encrypted user data is received by the DSS server(s) 204 and/or stored on the storage device(s) of the DSS 212. The full central portion of an exemplary private DSS, i.e., the "DSS server" 213, includes, but is not limited to, some server(s) 204 and some storage device(s) and/or components 212.];

a privacy preference database, comprising a list of allowed types of data packets for sharing during communication with the at least one user's device **[Moffat, para. 0097, Disclosed herein is a method of sharing data between a source of data and one or more recipients (e.g. a person's "friends") in which the data may only be viewed, understood and/or modified by the source, or the recipients, of the data, which includes: (a) protecting the privacy of the data from viewing, disclosure and/or exploitation by other parties, including the owners and/or operators of the system facilitating such data sharing; and (b) wherein the protecting of the privacy of the data is by data obfuscation and/or encryption prior to its transmission from the computing device(s) of the source, and by the clarification and/or decryption of that obfuscated and/or encrypted data upon the computing devices of the recipients.]**;

a communication module, to allow communication between the remote server and the at least one user's device **[Moffat, para. 0232, FIG. 1 illustrates a possible connection scheme between the DSS client that a user would utilize in order to access a DSS and a server of the DSS. A user's computing device 101 is connected to the Internet, or to some other electronic, digital or analog, data-sharing network. A program on the user's computer 101 (e.g. a browser program, a "stand-alone" program, etc.) exchanges messages and data with a DSS server by sending 102 properly addressed messages and/or data into the network 103. Those user messages and/or data arrive, via the network 103 at a DSS server 105. The DSS server receives data transmitted by the user's computer 101, and responds to requests for data by sending, when appropriate, messages and/or data back to the user's computer 101 via the Internet 103.]**; and

Moffat does not explicitly disclose, a processor, coupled to a response database and to the privacy preference database, wherein the processor is configured to instruct the remote server to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of data packets for sharing, and wherein the at least one data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device

However, Vaha-Sipila does disclose, a processor, coupled to a response database and to the privacy preference database, wherein the processor is configured to instruct the remote server to determine at least one data type for sharing of data

packet that is compatible with the list of allowed patterns of data packets for sharing, and wherein the at least one data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device

[Vaha-Sipila, para. 0046, 0070, FIG. 2 and FIG. 5, is a diagram of the components of privacy management platform for maintaining user privacy information, according to one embodiment. It is contemplated that the functions of these components may be combined in one or more components or performed by other components of equivalent functionality. In this embodiment, the privacy management platform 103 includes a controller 201, a communication module 203, an enforcement module 205, a data module 207, an identity management module 209, a transformation module 211, a call alert module 213 and a user interface module 215. The controller 201 oversees tasks performed by the various other modules. In addition, the privacy management platform 103 also accesses privacy policy data, privacy policy object data and local data from databases 115a-115c respectively. (Para. 0070), in FIG. 5, per steps 501-507 of process 500, the privacy management platform 103 determines to perform various actions responsive to the determined object. These may include determining to generate a prompt requesting an approval from a user of the device for the access, wherein the granting of the access is based, at least in part, on the approval (step 501); determining to generate an alert regarding the request (step 503); determining to apply at least one transformation to the local data, wherein the

access is granted to the transformed local data (step 505); and causing, at least in part, denial of the access to at least a portion of the local data (step 507). It is noted that the local data includes, at least in part, sensor data associated with the device.].

Moffat and Vaha-Sipila are in the same field of endeavor as they both are pertaining to means to management and protecting user privacy information.

Therefore, it would have been obvious to one of ordinary skill in the art before the effective date of claimed invention to modify the teachings of Moffat that relates to a data sharing system (DSS) is disclosed and seeks to ensure the privacy and security of users' personal information (Moffat, please abstract and para. 0031) with the teachings of Vaha-Sipila (Vaha-Sipila, para. 0046, 0070, FIG. 2 and FIG. 5) would enable Moffat with means to changing/ filtering any information or data that user may exchange with the a server through a privacy policy objective in order to protect the user's private information via a communication network.

Regarding claim 26. The combination of Moffat and Vaha-Sipila discloses the method of claim 24 above. Moffat does not explicitly disclose, a communication data pattern database, coupled to the processor and comprising at least one data pattern corresponding to sharing of at least one data packet from the user's device, wherein the processor is configured to modify data packets corresponding to requests for retrieval of data packets and communication data types that are not compatible with communication data patterns from a communication data pattern database

However, Vaha-Sipila does teach, a communication data pattern database, coupled to the processor and comprising at least one data pattern corresponding to sharing of at least one data packet from the user's device, wherein the processor is configured to modify data packets corresponding to requests for retrieval of data packets and communication data types that are not compatible with communication data patterns from a communication data pattern database **[Vaha-Sipila, para. 0046, 0053, and FIG, 2, is a diagram of the components of privacy management platform for maintaining user privacy information, according to one embodiment. It is contemplated that the functions of these components may be combined in one or more components or performed by other components of equivalent functionality. In this embodiment, the privacy management platform 103 includes a controller 201, a communication module 203, an enforcement module 205, a data module 207, an identity management module 209, a transformation module 211, a call alert module 213 and a user interface module 215. The controller 201 oversees tasks performed by the various other modules. In addition, the privacy management platform 103 also accesses privacy policy data, privacy policy object data and local data from databases 115a-115c respectively. (Para. 0053), in certain embodiments, the transformation module 211 applies a transformation to the local data such as to decrease the level of accuracy of a location, replacing the data with some other data to preserve privacy, or adjust a granularity of the data. The transformation module 211 determines a transformation function to perform based on a type of the local data 215c, the associated policy objects 215b and the privacy policy settings data 215a. In one example, the privacy policy**

may be determined based on sensitivity and primary usage. The sensitivity classification for the privacy policy may determine whether the information should be included in the transformed data.].

Moffat and Vaha-Sipila are in the same field of endeavor as they both are pertaining to means to management and protecting user privacy information.

Therefore, it would have been obvious to one of ordinary skilled in art before the effective filing date of claimed invention to modify the teachings of Moffat that provides and architecture for a data sharing system that facilitates the encryption, storage exchange and decryption of confidential and proprietary information (Please see abstract and para. 0022) with teachings of Vaha-Sipila (Vaha-Sipila, para. para. 0046, 0053, and FIG. 2) would enable Moffat with means to changing/ filtering any information or data that user may exchange with the a server through a privacy policy objective in order to protect the user's private information via a communication network.

Regarding claim 27. The combination of Moffat and Vaha-Sipila discloses the method of claim 26 above. Furthermore Moffat discloses, wherein data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory **[Moffat, para. 0235, FIG. 2 illustrates a possible structure of a private DSS of a type of this disclosure. A group of users 201, 202, 203 creates accounts within the DSS 213. These users interact with the DSS 213 through local DSS client programs ("DSS_CP's") 205, 206, 207 running on their respective**

computing devices 208, 209, 210. These DSS_CP's utilize the hardware and software resources of the users' computing devices 208, 209, 210 to communicate with, and exchange data with, the DSS server(s) 204. The DSS_CP's 205, 206, 207 only transmit encrypted versions of any user data transmitted into the Internet or other data sharing network 211. And, only encrypted user data is received by the DSS server(s) 204 and/or stored on the storage device(s) of the DSS 212. The full central portion of an exemplary private DSS, i.e., the "DSS server" 213, includes, but is not limited to, some server(s) 204 and some storage device(s) and/or components 212. (Para. 558), users are offered a number of "dynamic personal archives" as well as the "static," "write-once" archives discussed earlier. These dynamic personal archives allow users to create collections of data in which they can modify the contents over time through deletions, edits, etc. These dynamic archives can be implemented such that the frequent modification of the contents is facilitated. (Para. 0562), a user is able to change the attributes of one of his personal archives, for instance, changing a personal, private archive such as the one described above (dedicated to online tools for graphic illustrations) into a shared archive, either shared with a select group of other users or made public and accessible to any user. (Para. 0565), such private shared archives might be used for many purposes. For instance, they might be used to compile historical, or chronological, data related to an activity, the evolution of a business, a topic of interest (such as hang gliding), etc. (Para. 0567), such private forums might be used to create online marketplaces where various goods are offered for sale, or purchased, by a select set of users

who share a particular characteristic, e.g. an interest, a location, an employer, etc. For example, collectors of war-related postage stamps might organize a private forum wherein they could discuss stamps, and buy and sell their own stamps.].

Regarding claim 28. The combination of Moffat and Vaha-Sipila discloses the method of claim 26 above. Furthermore Moffat discloses, wherein at least the communication module and the processor are embedded on a single hardware component **[Moffat, para. 0232, FIG. 1 illustrates a possible connection scheme between the DSS client that a user would utilize in order to access a DSS and a server of the DSS. A user's computing device 101 is connected to the Internet, or to some other electronic, digital or analog, data-sharing network. A program on the user's computer 101 (e.g. a browser program, a "stand-alone" program, etc.).]**.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

A. **US PGPUB No. () to Ahmad** discloses, Systems and methods for automated content provisioning to a user device are disclosed herein. The system can include a memory including a user profile database containing information relating to a plurality of users and a content library database including a plurality of data packets.

B. **US PGPUB No. (2014/0031054) to Hanumantharayappa** discloses, a system and method for facilitating a remote connection between clients and servers.

C. US Patent No. (8,724,553) to Weniger discloses a method for route optimization of packet switched data transmissions between a first mobile node and a second mobile node in a mobile communication system comprising a plurality of access networks. The method comprises the step of transmitting return routability protocol packets and data packets. The return routability protocol packets and data packets are analysed, and at least part of an address comprised in headers of the return routability protocol packets and data packets is removed.

D. US Patent No. (7,231,027) to Schmid discloses a system and method to provide secure access across the untrusted public switched telephone network is described. The system and method can be initiated by a security policy defining actions to be taken based upon at least one attribute of the call.

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 MOHAMMAD S SHAMS whose telephone number is (571)272-3406. The examiner can normally be reached on Monday-Friday 8:00 AM-5:30 PM.

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, Kambiz Zand can be reached on (571)272-3811. 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 https://ppair-my.uspto.gov/pair/PrivatePair. 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.

/MOHAMMAD S SHAMS/
Examiner, Art Unit 2434

/SAMSON B LEMMA/
Primary Examiner, Art Unit 2498

Notice of References Cited	Application/Control No. 16/603,252	Applicant(s)/Patent Under Reexamination KOREN et al.	
	Examiner MOHAMMAD S SHAMS	Art Unit 2434	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-20140331054-A1	11-2014	HANUMANTHARAYAPPA; RAGHUNANDAN	H04L9/3234	713/176
*	B	US-20190034826-A1	01-2019	Ahmad; Zakariya	H04L63/0471	1/1
*	C	US-7231027-B2	06-2007	Schmid; Greg	H04L12/4633	379/188
*	D	US-8724553-B2	05-2014	Weniger; Kilian	H04W12/02	370/328
	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

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

*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.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/603,252	KOREN et al.
	Examiner	Art Unit
	MOHAMMAD S SHAMS	2434

CPC - Searched*		
Symbol	Date	Examiner
G06F21/6263, H04L63/0421, H04L63/0428	09/17/2020	M.S.S.

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
726	9	09/17/2020	

* 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
Applicant and Inventors Search	09/10/2020	M.S.S.
NPL, IP.com Search	09/17/2020	M.S.S.
EAST (Text and CPC) Search	09/22/2020	M.S.S.
Updated Applicant and Inventor(s) Search	01/23/2021	M.S.S.
Updated NPL, IP.com, and Google scholar search	01/23/2021	M.S.S.
Updated EAST (Text and CPC) Search	01/23/2021	M.S.S.

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

/MOHAMMAD S SHAMS/ Examiner, Art Unit 2434	/SAMSON B LEMMA/ Primary Examiner, Art Unit 2498

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/603,252	KOREN et al.
	Examiner	Art Unit
	MOHAMMAD S SHAMS	2434

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

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

CLAIM		DATE								
Final	Original	09/19/2020	01/24/2021							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	-	-							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	-	-							
	11	-	-							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	-	-							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							
	21	-	-							
	22	-	-							
	23	-	-							
	24	✓	✓							
	25	-	-							
	26	✓	✓							
	27	✓	✓							
	28	✓	✓							

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L8	736,618	(mask$3 obfuscat$3 conceal$3 disguis$3 hid$3 dissimulat$3 cover$3) with (data (data near2 packet) information)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/24 07:01
L9	331,370	(request$3 ask$3 seek$3 requir$3 solicit$3) with (shar$3 exchang$3 communicat$3 exchang$3) and (compatiblity agreeable matched incompatible acceptable)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/24 07:01
L10	62,853	L8 and L9	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/24 07:01
L11	3,128	L10 and ((characteristics traits identify$3 attributes pattern) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/24 07:01
L12	12	L11 and (privacy secrecy privateness confidentiality) near5 (data near2 packet) same (shar$3 exchang$3 communicat$3 exchang$3)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/24 07:01
S1	0	((("PRIVACY") near3 ("RATING") near3 ("LTD"))).AS,AANM.	USPAT	OR	ON	2020/09/10 17:21
S2	1	((("KOREN") near3 ("Yoseph"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/10 17:21
S3	1	((("WASSERMAN") near3 ("Yehonatan"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/10 17:21
S4	2	dynamic near2 management near2 private near2 data	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/10 17:22

S6	58,795	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/10 17:28
S7	1	S2 and S6	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/10 17:35
S8	1	S6 and S3	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/10 17:36
S9	28	(("20190347442") or ("20190182903") or ("20170325286") or ("10708978") or ("10212761") or ("20190342749") or ("10278065") or ("20180049023") or ("20170187758") or ("20100274859") or ("9781170") or ("20170230427") or ("20170230426") or ("10051018") or ("20190034060") or ("20190034826") or ("20190075140") or ("20160119330") or ("20190036775")).PN.	US-PGPUB; USPAT; USOCR; FPRS	OR	OFF	2020/09/12 16:34
S10	23	(("9954907") or ("20100064307") or ("20170041381") or ("10567479") or ("9197600") or ("10467552") or ("20140259147") or ("20180359811") or ("20040042414") or ("20090147772") or ("20170180504") or ("20190238655") or ("20160105416") or ("10306009") or ("8613026") or ("20170359420") or ("20120290844")).PN.	US-PGPUB; USPAT; USOCR; FPRS	OR	OFF	2020/09/12 16:45
S11	26	(("10402580") or ("8804966") or ("20090080661") or ("20190280986") or ("20170257143") or ("20190319932") or ("20180241727") or ("20150100488") or ("20180198757") or ("10491575") or ("10397335") or ("20200067884") or ("8254582") or ("20160219024")).PN.	US-PGPUB; USPAT; USOCR; FPRS	OR	OFF	2020/09/12 16:46
S12	77	S9 S10 S11	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/12 16:46

S15	2	"20130318347"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/12 16:59
S16	6	(("20090150968") or ("20070172066") or ("20100095119") or ("20040010467") or ("20100031335") or ("20100046749")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2020/09/12 17:08
S19	7	"2013318347"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2020/09/17 14:04
S20	2	"20130318347"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2020/09/17 14:04
S21	1	"20190149523"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/17 15:23
S22	10	"10348715"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/17 15:24
S23	6	"20170118638"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/17 15:28
S34	0	"16603252"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/18 09:31
S35	3	"10277614"	US-PGPUB; USPAT; USOCR;	OR	ON	2020/09/18 10:27

			FPRS; EPO			
S36	6	"20170118638"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/19 07:49
S37	3	"20150180839"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/19 07:50
S38	4	"20170054674"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/19 07:51
S39	2	"20160323305"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 11:04
S41	322,293	(request$3 ask$3 seek$3 requir$3 solicit$3) with (shar$3 exchang$3 communicat$3 exchang$3) and (compatiblity agreeable matched incompatible acceptable)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:36
S42	77	S41 and (privacy secrecy privateness confidentiality) near5 (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:37
S43	58,877	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:38
S44	588	"L1" and S43	US-PGPUB; USPAT; USOCR;	OR	ON	2020/09/21 15:38

			FPRS; EPO			
S45	27	S42 and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:39
S46	4	"20020015422"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:09
S47	4	"20140119380"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:13
S48	44	S42 and ((characteristics traits identify$3 attributes pattern) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:19
S49	39	S41 and (privacy secrecy privateness confidentiality) near5 (data near2 packet) same (shar$3 exchang$3 communicat$3 exchang$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:48
S50	2	S49 and (modify$3 alter$3 revis$3 adjust$3 amend$3 modulat$3 chang$3) near5 (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:51
S51	12	S42 and ((modificat$3 chang$3 alter$3 revis$3 adjust$3 amend$3) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 21:21
S56	0	S41 and ((modificat$3 chang$3 alter$3 revis$3 adjust$3 amend$3) with (data near2 packet)) same ((incompatible contridictory clash$3 unfit$3	US-PGPUB; USPAT; USOCR;	OR	ON	2020/09/21 21:58

		disagreeabble mismatched compatible) with (privacy security))	FPRS; EPO			
S57	0	S41 and (privacy secrecy privateness confidentiality) near5 (data near2 packet) same (incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:01
S58	0	S44 and (privacy secrecy privateness confidentiality) near5 (data near2 packet) same (incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:01
S59	31	S44 and (incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:02
S60	3,093	S41 and (incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:10
S61	475	S60 and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:10
S62	6	S61 and (privacy secrecy privateness confidentiality) near5 (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:12
S63	3,911	((outgoing transmit$4 send$3) with (data packet information)) same (privacy near4 (set$4 policy rule))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:25
S64	468	((outgoing transmit$4 send$3) with (data packet information)) same (privacy near4 (set$4 policy rule)) with (complian$2 comply$3 complies violat$3)	US-PGPUB; USPAT; USOCR;	OR	ON	2020/09/22 12:27

			FPRS; EPO			
S65	1,516	((outgoing transmit$4 send$3) with (data packet information)) same ((privacy security) near4 (set$4 policy rule)) with (complian$2 comply$3 complies violat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:28
S66	58,901	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:29
S67	88	S65 and S66	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:29
S68	5	S67 and ((modificat$3 chang$3 alter$3 revis$3 adjust$3 amend$3) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 13:54
S69	6	"20120005720"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 15:01
S70	6	"20120005720"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/19 12:45
S71	2	"20130318347"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/19 12:46
S72	2	"20090150968"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/19 13:26
S73	5	"20180082058"	US-PGPUB;	OR	ON	2021/01/20 11:45

			USPAT; USOCR; FPRS			
S74	1	"20180276375"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 11:45
S75	2	"20130318347"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 11:53
S77	60,667	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2021/01/20 12:56
S78	6	(("20090150968") or ("20070172066") or ("20100095119") or ("20040010467") or ("20100031335") or ("20100046749")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/20 12:56
S79	0	S77 and S78	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 12:56
S80	16	(("20200387637") or ("20190347442") or ("10778730") or ("20170325286") or ("20190182903") or ("10708978") or ("10212761") or ("20190342749") or ("20180049023") or ("10278065") or ("10785641") or ("20100274859") or ("20170187758") or ("9781170") or ("20170230427") or ("20170230426")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/20 13:00
S81	15	(("20190034060") or ("20040042414") or ("20190034826") or ("20160308907") or ("10051018") or ("20190075140") or ("20190036775") or ("20030135587") or ("9954907") or ("20160119330") or ("9749293") or ("20140331054") or ("10467552") or ("20140259147") or ("20120290844")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/20 13:00
S82	16	(("9197600") or ("20090080661") or ("20040143738") or ("20200356618") or ("20170041381") or ("8804966") or ("10567479") or ("20090147772") or	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/20 13:00

		("9660961") or ("20200084285") or ("8254582") or ("20170359420") or ("20170180504") or ("20200394246") or ("20190238655") or ("20160105416")).PN.				
S83	47	S80 S81 S82	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 13:01
S84	10	S83 and S77	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 13:01
S85	6	"20120005720"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/20 17:26
S86	32	"7676526"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 10:15
S87	4	"20140032228"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 10:40
S88	8	"20050066134"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 10:45
S92	4,644	(management governance monitor$3 plann$3) with (private encrpt$3 obfuscat$2) near2 data	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:09
S93	3,092	S92 and (server (remote near2 server) host) with (user client)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:11
S94	691	S93 and (read scanned allowed) with ((data near2 packet) file)	US-PGPUB; USPAT;	OR	ON	2021/01/21 17:17

			USOCR; FPRS			
S95	691	S92 and (server (remote near2 server) host) with (user client) and ((read scanned allowed) with ((data near2 packet) file))	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:18
S96	69	S95 and (G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:20
S97	3	S96 and (restricted modified controlled banned unread) with (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:30
S98	49	S96 and (restricted modified controlled banned unread) with data	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 17:32
S99	11	"9477836"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 18:17
S100	24	"9609025"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 19:29
S101	4	"20170098215"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 19:35
S103	22	S98 and (@ad<"20170409")	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/21 22:16
S104	17,199	(data near2 packet) with ("not read" restricted modified controlled banned unread)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/22 18:18

S105	67	S104 and (privacy secrecy privateness confidentiality) near5 (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/22 18:20
S106	20	S105 and (G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/22 18:20
S107	1	"20120222083"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/22 18:55
S108	16	(("20200387637") or ("20190347442") or ("10778730") or ("20170325286") or ("20190182903") or ("10708978") or ("10212761") or ("20190342749") or ("20180049023") or ("10278065") or ("10785641") or ("20100274859") or ("20170187758") or ("9781170") or ("20170230427") or ("20170230426")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/23 10:14
S109	15	(("20190034060") or ("10051018") or ("20040042414") or ("20160308907") or ("20190034826") or ("20190075140") or ("20190036775") or ("20030135587") or ("9954907") or ("20160119330") or ("9749293") or ("20140331054") or ("10467552") or ("20140259147") or ("20120290844")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/23 10:15
S110	17	(("9197600") or ("20090080661") or ("20200356618") or ("20040143738") or ("20170041381") or ("8804966") or ("10567479") or ("20090147772") or ("9660961") or ("8254582") or ("20200084285") or ("20170359420") or ("20170180504") or ("20200394246") or ("20190238655") or ("20200358858") or ("20160105416")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2021/01/23 10:15
S111	48	S108 S109 S110	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 10:16
S112	10	S111 and (G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT;	OR	ON	2021/01/23 10:16

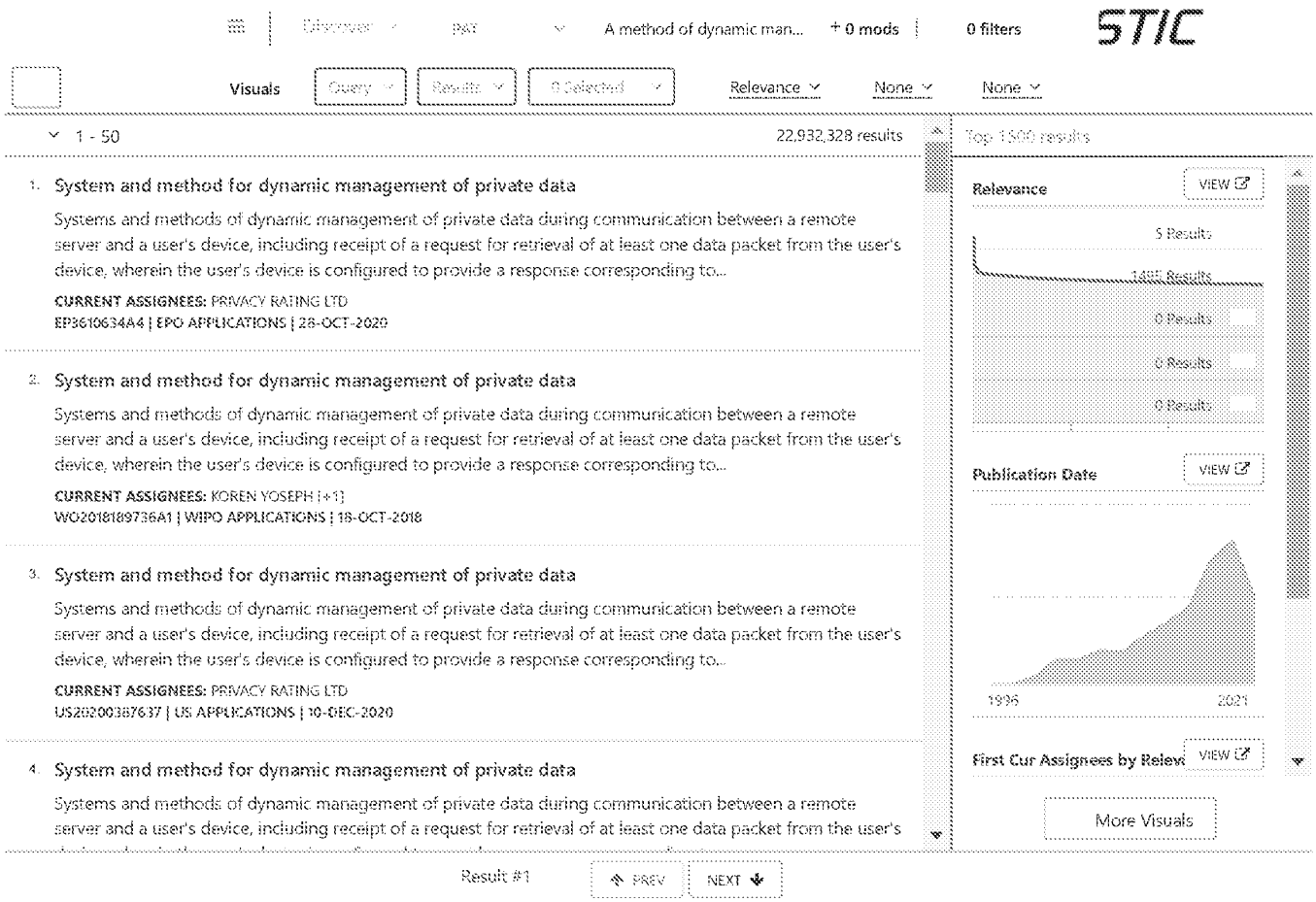
			USOCR; FPRS			
S113	2	((("PRIVACY") near3 ("RATING") near3 ("LTD"))).AS,AANM.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:03
S114	7	((("KOREN") near3 ("Yoseph"))).INV.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:04
S115	7	((("WASSERMAN") near3 ("Yehonatan"))).INV.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:04
S116	736,618	(mask$3 obfuscat$3 conceal$3 disguis$3 hid$3 dissimulat$3 cover$3) with (data (data near2 packet) information)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:07
S117	60,694	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:09
S118	7,323	S116 and S117	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:10
S119	331,370	(request$3 ask$3 seek$3 requir$3 solicit$3) with (shar$3 exchang$3 communicat$3 exchang$3) and (compatiblity agreeable matched incompatible acceptable)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:10
S120	62,853	S116 and S119	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:11
S121	3,128	S120 and ((characteristics traits identify$3 attributes pattern) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:12

S122	12	S121 and (privacy secrecy privateness confidentiality) near5 (data near2 packet) same (shar$3 exchang$3 communicat$3 exchang$3)	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:14
S123	10	S122 and S117	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2021/01/23 11:15

EAST Search History (Interference)

<This search history is empty>

1/24/2021 7:14:26 AM
C:\Users\mshams\Documents\EAST\Workspaces\16603252.wsp


Discover
PAT
A method of dynamic man...
+ 0 mods
0 filters
STIC
Visuals
Query
Results
0 Selected
Relevance
None
None
1 - 50
22,932,328 results
Top 1500 results
1. System and method for dynamic management of private data
Systems and methods of dynamic management of private data during communication between a remote server and a user's device, including receipt of a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to...
CURRENT ASSIGNEES: PRIVACY RATING LTD
EP3610634A4 | EPO APPLICATIONS | 28-OCT-2020
2. System and method for dynamic management of private data
Systems and methods of dynamic management of private data during communication between a remote server and a user's device, including receipt of a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to...
CURRENT ASSIGNEES: KOREN YOSEPH [+1]
WO2018189736A1 | WIPO APPLICATIONS | 18-OCT-2018
3. System and method for dynamic management of private data
Systems and methods of dynamic management of private data during communication between a remote server and a user's device, including receipt of a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to...
CURRENT ASSIGNEES: PRIVACY RATING LTD
US20200387637 | US APPLICATIONS | 10-DEC-2020
4. System and method for dynamic management of private data
Systems and methods of dynamic management of private data during communication between a remote server and a user's device, including receipt of a request for retrieval of at least one data packet from the user's
Relevance
VIEW
5 Results
1495 Results
0 Results
0 Results
0 Results
Publication Date
VIEW
1996
2021
First Cur Assignees by Relev
VIEW
More Visuals
Result #1
PREV
NEXT

A multi-level monitoring approach for the **dynamic management** of **private** iaas platforms

R Garcia-Carmona, F Cuadrado, Á Navas... - Journal of Internet ..., 2013 - eecs.qmul.ac.uk

... To properly implement a **dynamic management** system in a cloud environment it is imperative to have ... propose an information model that offers a multi-level view of a **private** IaaS cloud ... between consumers and providers, and enables the correlation of the collected **data** to have ...

☆ 99 Cited by 5 Related articles All 5 versions »

Dynamic virtual **private** network system and methods

U Chandrashekhar, ML El-Sayed, KJ Johnson... - US Patent ..., 2010 - Google Patents

... the field of communications systems and, more particularly, the invention relates to a system and method for **dynamic management** of Internet ... a central location using the Internet or an Internet Service Provider's (ISP's) public, shared IP network to securely transmit **private data** ...

☆ 99 Cited by 210 Related articles All 4 versions »

Dynamic private network

GP Mattathil - US Patent 6,807,169, 2004 - Google Patents

... of bandwidth another method for building **private** networks can be implemented, one which the present inventor terms "**dynamic private** network" (DPN) ... Such special service devices 12 e typically require a much lower **data** transfer rate than systems like the computers 12 d and ...

☆ 99 Cited by 119 Related articles All 4 versions »

Content recommendation system based on **private dynamic** user profile

T Chen, WL Han, HD Wang, YX Zhou... - ... on machine learning ..., 2007 - ieeexplore.ieee.org

... It is a hotspot in the research area of content **management** on WWW ... an agent-based personalized recommendation method called Content REcommendation System based on **private Dynamic** User Profile ... The system collects and mines the **private data** of user at the client side ...

☆ 99 Cited by 98 Related articles All 4 versions

Virtual infrastructure **management** in **private** and hybrid clouds

B Sotomayor, RS Montero, IM Llorente... - IEEE Internet ..., 2009 - ieeexplore.ieee.org

... not found in other cloud systems, such as advance reserva- tions (ARs) and resource preemption, which are particularly relevant for **private** clouds ... org), meet many of the VI **management** require- ments we outlined earlier, providing features such as **dynamic** placement and ...

☆ 99 Cited by 1415 Related articles All 24 versions »

Verifiable **management** of **private data** under byzantine failures

E Kokoris-Kogias, EC Alp, SD Siby, N Gailly... - Cryptol. ePrint Arch ..., 2018 - aliquantor.at

... We introduce Calypso, a decentralized framework for au- ditable **management** of **private data** while maintaining fair- ness and confidentiality (see Section 3). Calypso enables **dynamic** updates to access-control rules without compromis- ing security ...

☆ 99 Cited by 8 Related articles »

Automated generation of **dynamic data** entry user interface for relational database **management** systems

JN Kesler - US Patent 7,062,502, 2006 - Google Patents

US7062502B1 - Automated generation of **dynamic data** entry user interface for relational database **management** systems - Google Patents. Automated generation of **dynamic data** entry user interface for relational database **management** systems. Download PDF Info ...

☆ 99 Cited by 1125 Related articles All 2 versions »

Automated generation of **dynamic data** entry user interface for relational database **management** systems

JN Kesler - US Patent 7,401,094, 2008 - Google Patents

US7401094B1 - Automated generation of **dynamic data** entry user interface for relational database **management** systems - Google Patents. Automated generation of **dynamic data** entry user interface for relational database **management** systems. Download PDF Info ...

☆ 99 Cited by 1032 Related articles All 2 versions »

Private data aggregation with groups for smart grids in a **dynamic** setting using CRT

Z Erkin - 2015 IEEE international workshop on information ..., 2015 - ieeexplore.ieee.org

... The **dynamic** nature of the smart meters, requirement for working in fine granularity and limited ... [7] M. Kohlweiss and G. Danezis, "Differentially **private** billing with ... energy-metering via homomorphic encryption," in 6th Workshop on Security and Trust **Management** (STM 2010), ser ...

☆ 99 Cited by 22 Related articles All 4 versions

Private and **dynamic** time-series **data** aggregation with trust relaxation

I Leontiadis, K Elkhiyaoui, R Molva - International Conference on ..., 2014 - Springer

... Our scheme extends Joye and Libert scheme [7] through two major enhancements : – No key dealer: Our scheme does not require a trusted key dealer that might get individual **private data** samples. – **Dynamic** group **management**: In the Joye and Libert scheme [7], each join or ...

☆ 99 Cited by 32 Related articles All 11 versions »

Related searches

private data **aggregation** dynamic **setting**

iaas platforms dynamic management

infrastructure management private **and hybrid clouds**

dynamic data **entry user interface**

dynamic **resource** management

time series data private **aggregation**

monitoring approach dynamic management

private data **aggregation smart grids**

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
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 displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 16/603,252	Filing Date 10/07/2019	☐ To be Mailed

ENTITY: ☑ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ 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 $100 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $460 =	
☐ 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))					
* 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)			
AMENDMENT	12/27/2020	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 $100 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $480 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
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 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ 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.	SLIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/SHANDA E ROSS/
*** 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.

Attorney Docket No.: P-566702-US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	KOREN, Yoseph et al.	Examiner:	Shams, Mohammad S
Serial No.:	16/603,252	Group Art Unit:	2434
Filed:	October 07, 2019	Confirmation No.:	6147
Title:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA		

AMENDMENT

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

Sir/Madam:

This Amendment is being filed in response to the Office Action mailed September 28, 2020 by the United States Patent and Trademark Office in connection with the above-identified Application. A response to the September 28, 2020 Office Action is due December 28, 2020. Accordingly, this paper is being timely filed.

Kindly amend the above-identified application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page **2** of this paper.

Remarks/Arguments begin on page **8** of this paper.

AMENDMENTS TO THE CLAIMS

Please amend claims 1, 4, 5, 7, 12, 15, 17, 18 and 24.

This listing of claims will replace all prior versions, and listings, of claims in this application:

Listing of Claims:

1. **(Currently Amended)** A method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request;

determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device;

receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication;

modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference; and

maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

2. (Original) The method of claim 1, wherein the communication data type of the at least one data packet is determined from metadata of communication with the remote server.

3. (Original) The method of claim 1, further comprising:

determining, by the user's device, at least one communication data pattern of at least one data packet corresponding to the received request; and

modifying data packets corresponding to requests for sharing of responses corresponding to at least one data pattern, that are not compatible with the received privacy preference,

wherein the privacy preference comprises a list of allowed data patterns for sharing during communication.

4. **(Currently Amended)** The method of claim 3, wherein the communication data pattern is determined based on a range selected from a group consisting of: data packet frequency, data packet size, data packet speed, data packet count, data packet ratio compared to other data type flow, data packet ~~repentance~~ repetition, and data packet order.

5. **(Currently Amended)** The method of claim 1, wherein the communication data type is determined based on data packet characteristics selected from a group consisting of: data packet header, data packet footer, version number, IP (Internet Protocol) address, HTTPS (HyperText Transfer Protocol Secure), file extension, encryption method, encoding method, keywords, driver, and communication protocol.

6. (Canceled)

7. **(Currently Amended)** The method of claim 1, further comprising:

determining, by the remote server, [[the]] a communication data pattern of the at least one data packet of the received request; and

linking at least one response from the user's device to a type of data packet from the user's device, wherein the linking is based on the communication data type and communication data pattern of the at least one response.

8. (Original) The method of claim 1, further comprising:

identifying a response corresponding to a request for sharing of data packets, wherein the identified response is not compatible with the received privacy preference; and

providing a response with at least one modified data packet corresponding to the request for sharing types of data packets.

9. (Original) The method of claim 8, wherein the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

10. (Canceled)

11. (Canceled)

12. **(Currently Amended)** A method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request;

determining, by the remote server, at least one communication data pattern corresponding to the received request, wherein the at least one communication data pattern is determined in accordance with a behavior range of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device;

receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data patterns for sharing during communication;

modifying data packets corresponding to requests for sharing of responses and corresponding data patterns that are not compatible with the received privacy preference; and

maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

13. (Original) The method of claim 12, wherein the communication data pattern of the at least one response is determined from metadata of communication with the remote server.

14. (Original) The method of claim 12, further comprising:

determining, by the remote server, the communication data type of the at least one data packet of the received request; and

modifying data packets corresponding to requests for sharing of responses and corresponding data patterns, corresponding to at least one communication data packet type, that are not compatible with the received privacy preference,

wherein the privacy preference comprises a list of allowed data packet types for sharing during communication.

15. (**Currently Amended**) The method of claim 14, wherein the communication data type is determined based on data packet characteristics selected from a group consisting of: data packet header, data packet footer, version number, IP (Internet Protocol) address, HTTPS (HyperText Transfer Protocol Secure), file extension, encryption method, encoding method, keywords, driver, and communication protocol.

16. (Canceled)

17. (**Currently Amended**) The method of claim 12, wherein the user's device is in communication with an external database with at least one communication data pattern corresponding to a request for sharing of data packets from the user's device, and wherein [[the]] at least one data pattern compatible with the received request is determined from the database.

18. (**Currently Amended**) The method of claim 12, further comprising:

determining, by the remote server, [[the]] a type of the at least one data packet of the received request; and

linking at least one data pattern to a type of data packet from the user's device, wherein the linking is based on the communication data type and the communication data pattern of the at least one response.

19. (Original) The method of claim 12, further comprising:

identifying a communication data pattern corresponding to a request for sharing of data packet types, wherein the identified data pattern is not compatible with the received privacy preference; and

providing a response with at least one modified data packet corresponding to the request for sharing types of data packets.

20. (Original) The method of claim 19, wherein the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

21. (Canceled)

22. (Canceled)

23. (Canceled)

24. (**Currently Amended**) A system for dynamic management of private data during communication between a remote server and at least one user's device, the system comprising:

a communication data type database, comprising at least one communication data type corresponding to sharing of at least one data packet from the user's device;

a privacy preference database, comprising a list of allowed types of data packets for sharing during communication with the at least one user's device;

a communication module, to allow communication between the remote server and the at least one user's device; and

a processor, coupled to [[the]] a response database and to the privacy preference database,

wherein the processor is configured to instruct the remote server to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of data packets for sharing, ~~and~~ wherein the at least one data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device.

25. (Previously Canceled)

26. (Original) The system of claim 24, further comprising a communication data pattern database, coupled to the processor and comprising at least one data pattern corresponding to sharing of at least one data packet from the user's device, wherein the processor is configured to modify data packets corresponding to requests for retrieval of data packets and communication data types that are not compatible with communication data patterns from a communication data pattern database.

27. (Original) The system of claim 26, wherein data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

28. (Original) The system of claim 26, wherein at least the communication module and the processor are embedded on a single hardware component.

REMARKS

The present response is intended to be fully responsive to all points of objection and/or rejection raised by the Examiner and is believed to place the application in condition for allowance.

Applicants assert that the present invention is new, non-obvious and useful. Prompt consideration and allowance of the claims is respectfully requested.

Status of Claims

Claims 1-5, 7-9, 12-15, 17-20, 24 and 26-28 are pending.

Claims 5 and 15 have been objected to.

Claims 1-5, 7-9, 12-15, 17-20, 24 and 26-28 have been rejected.

Claims 1, 4, 5, 7, 12, 15, 17, 18 and 24 have been amended.

Applicants respectfully assert that the amendments to the claims add no new matter.

Claim Objections

In the Office Action, the Examiner objected to claims 5 and 15 because of alleged informalities. Claims 5 and 15 have been amended in order to cure these informalities. Accordingly, Applicants request withdrawal of the objection.

CLAIM REJECTIONS

35 U.S.C. § 112 Rejections

In the Office Action, the Examiner rejected claims 4, 7, 17, 18 and 24 under 35 U.S.C. § 112(b), as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicants regard as the invention.

Accordingly, claim 4 has been amended to recite “data packet repetition”, to correct a typographic error.

Claims 7, 17, 18 and 24 have been amended to overcome the antecedent basis deficiencies noted by the Examiner.

Applicants respectfully assert that these amendments render claims 4, 7, 17, 18 and 24 proper under 35 U.S.C. § 112(b) and request that the rejections be withdrawn.

35 U.S.C. § 103 Rejections

In the Office Action, the Examiner rejected claims 1-5, 7-9, 12-15, 17-20, 24 and 26-28 under 35 U.S.C. § 103, as being unpatentable over Moffat (US Patent Publication No. 2013/0318347) in view of McGloin et al. (US Patent Publication No. 2012/0005720).

Applicants respectfully traverse the rejection in view of the remarks that follow.

Moffat fails to teach determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device, as recited in amended independent claim 1.

According to paragraph [0221] of Moffat, the data sharing system (DSS) determines the relevance of data packets of user data with respect to the type of media, e.g. the media-specific "page" or "section" of the "user interface" being viewed by a user on his local computing device, and also its date of creation and/or uploading. The relevance of a packet of user data might also be affected by whether or not it is related to some other piece of user data, such as a comment on a photo, i.e. metadata related to the content of the data packet. Thus, Moffat directly analyses and inspects the content of data packets of the user's data to determine relevance to the user's privacy preference, for example media with a comment on a photo as indicated in paragraph [0221] of Moffat. Accordingly, Moffat cannot teach or suggest determining communication data type while the content is not read, for continued operation by the user's device in real time.

In contrast, in the present claims the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during

communication between the remote server and the user's device. For example, in the embodiment described in paragraph [062] of the present application, determination of data type does not read and concern the actual content of the data packet even if the content is encrypted.

Applicants assert that McGloin et al. is also silent as to determination of the at least one communication data type carried out in accordance with characteristics of the communication data packet, wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device as recited at least in amended independent claim 1, and, therefore, cannot cure the deficiencies of Moffat.

Accordingly, Applicants respectfully assert that amended independent claim 1 is allowable over the above cited references. Similar arguments apply to independent claims 12 and 24, *mutatis mutandis*.

Regarding claim 2, Applicant notes that while Moffat mentions metadata in paragraphs [0500]-[0501], this refers to user defined privacy preferences and not metadata as the characteristics and/or behavior of the data packet of the present application. Specifically, Moffat indicates in paragraph [0500]:

> Metadata may include such things as: which mode of a multi-modal user interface (UI) was last selected by the user; the maximum age of the user data which the user wishes to see included in the collections of data presented to the user by the DSS client's UI; which elements of user data the user has specified to be hidden; for which presentation template(s) (or "skin(s)") has the user expressed a preference; etc. (emphasis added)

Each of claims 2-5, 7-9, 13-15, 17-20 and 26-28 depends, directly or indirectly, from one of amended independent claims 1, 12 and 24, and, therefore, includes all the limitations of that claim. Therefore, Applicants respectfully assert that claims 2-5, 7-9, 13-15, 17-20 and 26-28 are likewise allowable.

Accordingly, Applicants respectfully request that the rejection of claims 1-5, 7-9, 12-15, 17-20, 24 and 26-28 under 35 U.S.C. § 103 be withdrawn.

Conclusion

In view of the foregoing amendments and remarks, Applicants assert that the pending claims are allowable. Their favorable reconsideration and allowance is respectfully requested.

Should the Examiner have any question or comment as to the form, content or entry of this Amendment, the Examiner is requested to contact the undersigned at the telephone number below. Similarly, if there are any further issues yet to be resolved to advance the prosecution of this application to issue, the Examiner is requested to telephone the undersigned counsel.

To the extent that there are any fees associated with this filing that are due but are not paid or are not able to be paid by a credit card mentioned elsewhere in this document, Applicants authorize the U.S. Patent and Trademark Office to charge any such fees to deposit account No. 60-2041.

Respectfully submitted,

/Caleb Pollack/

_____

Caleb Pollack
Attorney/Agent for Applicant(s)
Registration No. 37,912

Dated: December 27, 2020

Pearl Cohen Zedek Latzer Baratz LLP
1500 Broadway, 12th Floor
New York, New York 10036
Tel: (646) 878-0800
Fax: (646) 878-0801

Electronic Acknowledgement Receipt

EFS ID:	41491182
Application Number:	16603252
International Application Number:	
Confirmation Number:	6147
Title of Invention:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA
First Named Inventor/Applicant Name:	Yoseph KOREN
Customer Number:	49443
Filer:	Caleb Pollack/Sigal Vegh
Filer Authorized By:	Caleb Pollack
Attorney Docket Number:	P-566702-US
Receipt Date:	27-DEC-2020
Filing Date:	07-OCT-2019
Time Stamp:	09:38:10
Application Type:	U.S. National Stage under 35 USC 371

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		P-566702-US-U-RESOA-27DEC20.pdf	155324 c4cd0c2090be71d375e854737aac1b54835a68d4	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	11
Warnings:			
Information:			
	Total Files Size (in bytes):	155324	

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.

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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/603,252	10/07/2019	Yoseph KOREN	P-566702-US

CONFIRMATION NO. 6147

49443
Pearl Cohen Zedek Latzer Baratz LLP
1500 Broadway
12th Floor
New York, NY 10036

PUBLICATION NOTICE

OC000000121934768

Title:SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

Publication No.US-2020-0387637-A1
Publication Date:12/10/2020

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 Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/08a (07-09)
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.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	1	of	2

Complete if Known	
Application Number	**16/603,252**
Filing Date	**October 07, 2019**
First Named Inventor	**KOREN, Yoseph**
Art Unit	**2434**
Examiner Name	**Shams, Mohammads**
Attorney Docket Number	**P-566702-US**

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A	US-9,609,025	Mar. 28, 2017	Betzler Boas et al.	
	B	US-9,477,836	Oct. 25, 2016	Rambam Shishir Krovvidi et al.	
	C	US-2017/098215	Apr. 6, 2017	Brotsky Daniel C	
	D	US-2012/0222083	Aug. 30, 2012	VAHA-SIPLA et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	E	WO 2013 103782	Jul. 11, 2013	3M Innovative Properties Company		☐
	F	WO 2014 031041	Feb. 27, 2014	Ericsson Telefon AB et al.		☐
						☐
						☐
						☐
						☐
						☐
						☐

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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 2 hours 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, 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 (1-800-786-9199) and select option 2.

PTO/SB/08b (07-09)
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.

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*				***Complete if Known***	
				Application Number	**16/603,252**
				Filing Date	**October 07, 2019**
				First Named Inventor	**KOREN, Yoseph**
				Art Unit	**2434**
(use as many sheets as necessary)				Examiner Name	**Shams, Mohammads**
Sheet	**2**	of	**2**	Attorney Docket Number	**P-566702-US**

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (where appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	G	Supplementary European Search Report Application No. EP 18785029 dated Sep. 15, 2020	☐
	H	PCT IPRP International Application No. PCT/IL2018050359. International Filing Date Mar. 28, 2018	☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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 2 hours 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, 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 (1-800-786-9199) and select option 2.

Attorney Docket No.: P-566702-US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	KOREN, Yoseph et al.	Examiner:	Shams, Mohammads
Serial No.:	16/603,252	Group Art Unit:	2434
Filed:	October 07, 2019	Confirmation No.:	6147
Title:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA		

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

Sir/Madam:

INFORMATION DISCLOSURE STATEMENT

Pursuant to 37 C.F.R. §§1.56, 1.97 and 1.98, this Information Disclosure Statement includes Form PTO/SB/08:

1. ☒ listing documents including patents, publications and other information for consideration by the Examiner, however, since the subject application was filed after June 30, 2003, copies of United States patents and/or United States patent application publications are not included in this information disclosure statement; and/or
2. ☐ listing documents including patents, publications and other information that have been previously cited or submitted to the Patent Office in prior application U.S. Patent application No. , filed which is properly identified and relied on for an earlier effective filing date under 35 U.S.C. 120 for consideration by the Examiner; however, in accordance with 37 C.F.R. 1.98(d), copies of such documents are not included in this information disclosure statement; and/or
3. ☐ listing documents including patents, publications, and other information for consideration by the Examiner, copies of which are included with this information disclosure statement;
4. ☒ listing documents including patents, publications, and other information for consideration by the Examiner, which were cited in a communication from a foreign patent office in a counterpart foreign application, copies of which are included with this information disclosure statement.

The information herein cited is only in fulfillment of Applicant(s) duty of candor in disclosing all information brought to Applicant(s) attention. This submission does not represent that a search has been made or that no better art exists and does not constitute an admission that each or all of the listed documents are material or constitute "prior art". If it should be determined that any of the listed documents do not constitute "prior art" under United States law, Applicant(s) reserve the right to present to the office the relevant facts and law regarding the appropriate status of such documents.

Applicant(s) further reserve(s) the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

In accordance with MPEP Sections 609 and 707.05(b), it is requested that each and every document cited (including any cited in applicant's specification which is not repeated on the attached Form PTO-1449) be given thorough consideration and that it be cited of record in the prosecution history of the present application by initialing on Form PTO-1449. Such initialing is requested even if the Examiner does not consider it to be prior art for any reason, or even if the Examiner does not believe that the guidelines for citation have been fully complied with. This is requested so that each document becomes listed on the face of the patent issuing on the present application and is evidence that the Examiner has considered the document. Neither the submission of the Information Disclosure Statement nor the content of any document cited herein constitutes a disclaimer of claim scope or an admission that any item submitted constitutes prior art.

This Information Disclosure Statement is being filed:

I) ☐ Within three (3) months of filing the subject Application or entry of the subject Application into the national stage; or before mailing of the first Office Action on the merits of the subject Application, whichever event occurs last; or before mailing of the first Office Action on the merits after filing a request for continued examination, pursuant to of 37 C.F.R §1.97 (b); or

II) ☒ After the period specified in (I) but before the mailing date of either a final Official Action under 37 C.F.R §1.113 or a notice of allowance under 37 C.F.R §1.311 whichever occurs first and;

1. ☐ the undersigned hereby states that each item of information listed on the Form PTO-1449 was either (i) cited in a communication from a foreign patent office in a counterpart foreign application not more than three (3) months prior to the filing of this Information Disclosure Statement or (ii) not cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, not known to any individual designated in §1.56(c) more than three (3) months prior to the filing of this information disclosure statement; or

2. ☒ the fee in the amount of $130 (Small Entity) under 37 C.F.R §1.17 (p) is being paid by credit card (note deposit account information below in the event of lack of credit card payment).

III) ☐ After the period in (I) and (II) but before the payment of the issue fee and,

1. The undersigned hereby states:

a) ☐ that each item of information cited on the form PTO-1449 was first cited in a communication from a foreign Patent Office in a counterpart foreign

application not more than three (3) months prior to the filing of this Information Disclosure Statement; or

b) ☐ that no items of information contained in Form PTO-1449 were cited in a communication from a foreign patent office in a counterpart foreign application, and to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement; and

2. ☐ The Petition fee in the amount of $260 (Large Entity) under 37 C.F.R §1.17 is being paid by credit card (note deposit account information below in the event of lack of credit card payment).

To the extent that there are any fees associated with this filing that are due but are not paid or are not able to be paid by a credit card mentioned elsewhere in this document, Applicants authorize the U.S. Patent and Trademark Office to charge any such fees to deposit account No. **50-3355**..

Respectfully submitted,

/Devorah N. Livneh/
Devorah N. Livneh
Attorney/Agent for Applicant(s)
Registration No. 71,347

Dated: December 2, 2020

Pearl Cohen Zedek Latzer Baratz LLP
1500 Broadway, 12th Floor
New York, New York 10036
Tel: (646) 878-0800
Fax: (646) 878-0801

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING TRANSMITTAL OF COPY OF INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (CHAPTER I OF THE PATENT COOPERATION TREATY)
(PCT Rule 44bis.1(c))

To:

FRYDMAN, Idan
Pearl Cohen Zedek Latzer Baratz
P.O. Box 7198
6107121 Tel Aviv
ISRAËL

Date of mailing *(day/month/year)*
24 October 2019 (24.10.2019)

Applicant's or agent's file reference
P-566702-PC

IMPORTANT NOTICE

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/IL2018/050359	28 March 2018 (28.03.2018)	09 April 2017 (09.04.2017)

Applicant
KOREN, Yoseph

The International Bureau transmits herewith a copy of the international preliminary report on patentability (Chapter I of the Patent Cooperation Treaty)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 82 70

Authorized officer
Simin Baharlou

e-mail: pct.team9@wipo.int

Form PCT/IB/326 (January 2004)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference P-566702-PC	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/IL2018/050359	International filing date *(day/month/year)* 28 March 2018 (28.03.2018)	Priority date *(day/month/year)* 09 April 2017 (09.04.2017)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant KOREN, Yoseph		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	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 Article 35(2) 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

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 15 October 2019 (15.10.2019)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Simin Baharlou e-mail: pct.team9@wipo.int

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
PEARL COHEN ZEDEK LATZER BARATZ
P.O. Box 7198
Tel Aviv 6107121
Israel

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	12 Jul 2018
Applicant's or agent's file reference P-566702-PC	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/IL2018/050359	28 Mar 2018	09 Apr 2017

International Patent Classification (IPC) or both national classification and IPC
IPC (2018.01) H04L 29/12

Applicant
KOREN Yoseph

1. This opinion contains indications relating to the following items:

- [x] 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
- [x] Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- [ ] Box No. VI Certain documents cited
- [ ] Box No. VII Certain defects in the international application
- [x] 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:	Date of completion of this opinion	Authorized officer
Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Facsimile No. 972-2-5651616	10 Jul 2018	MARCOWITZ Noam Telephone No. 972-2-5651735

Form PCT/ISA/237 (cover sheet) (January 2015)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IL2018/050359

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   [X] 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 43*bis*.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:

   a. [ ] forming part of the international application as filed:

      [ ] in the form of an Annex C/ST.25 text file.

      [ ] on paper or in the form of an image file.

   b. [ ] furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. [ ] furnished subsequent to the international filing date for the purposes of international search only:

      [ ] in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      [ ] on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

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 forming part of 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/IL2018/050359

Box No. V **Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims		YES
	Claims	1-28	NO
Inventive step (IS)	Claims		YES
	Claims	1-28	NO
Industrial applicability (IA)	Claims	1-28	YES
	Claims		NO

2. Citations and explanations:

1. Reference is made to the following documents:

D1: WO2013103782

2. NOVELTY

Notwithstanding the observation regarding lacks of support, as noted at box VIII , it is determined that The subject-matter of claims 1, 2, 13, is not novel as being anticipated by D1 and therefore does not comply with PCT Article 33(2).
Regarding claim 1, D1 discloses a method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:
receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request (see ¶ 78, 232);
determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request (see ¶ 221, 494) ;
receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication (see ¶ 149, 221)
modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference (see ¶ 804) ; and
maintaining communication between the remote server and the user's device,with sharing of the modified data packets (see ¶ 804).

Thus, taking into account said observation regarding lacks of clarity mentioned above, it is maintained that D1 deprives novelty from the subject matter of said claim.

Regarding claims 2, 13, D1 is further disclosing that the communication data type of the at least one data packet is determined from metadata of communication with the remote server (see ¶ 499-501).

3. INVENTIVE STEP
The present application does not meet the criteria of Article 33 (1) PCT, because the subject-matter of claims 6-13, 16, 22-29, 32, does not involve an inventive step in the sense of Article 33(3) PCT.

Regarding claims 3-12, 14-28, Skilled person would consider as obvious possibility to improve the data security by monitoring the packets traffic for detecting an abnormal traffic pattern, as suggested by those claims. Said traffic monitoring would not involve any surprising effect in respect to the problem of privacy protection, nor would it supplement special contribution in respect to the solution which recited by independent claim 1 and disclosed in D1, namely, inspecting packets content according to the user privacy preferences. It is pointed out that the examples which given in the supporting disclosure in relation to the 'pattern' monitoring are concerning with cyber threats, such as denial of service attacks, and not actually with the specific problem of protecting the user privacy. Thereby, it could be argue that employing the user privacy preferences in respect to the monitoring of the traffic pattern would not have any special advantage.
Therefore, these claims subject matter lack inventive step.

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IL2018/050359

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Claim 1 is not properly supported by the specifications, contrary to article 5. Said claim recites that the communication data type is determined by a remote server, whereas the disclosure describes that said determination is performed by the user device.

Electronic Patent Application Fee Transmittal

Application Number:	16603252
Filing Date:	07-Oct-2019
Title of Invention:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA
First Named Inventor/Applicant Name:	Yoseph KOREN
Filer:	Devorah N Livneh/Laura Saporta
Attorney Docket Number:	P-566702-US

Filed as Small Entity

Filing Fees for U.S. National Stage under 35 USC 371

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($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	130	130
		Total in USD ($)		**130**

Electronic Acknowledgement Receipt

EFS ID:	41280821
Application Number:	16603252
International Application Number:	
Confirmation Number:	6147
Title of Invention:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA
First Named Inventor/Applicant Name:	Yoseph KOREN
Customer Number:	49443
Filer:	Devorah N Livneh/Laura Saporta
Filer Authorized By:	Devorah N Livneh
Attorney Docket Number:	P-566702-US
Receipt Date:	03-DEC-2020
Filing Date:	07-OCT-2019
Time Stamp:	04:45:02
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$130
RAM confirmation Number	E2020B3546043634
Deposit Account	602041
Authorized User	Laura Saporta
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 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		P-566702-US-U-IDS.pdf	72237 e75cc3ca9543d4270ca1ce6251b0e14ea093b640	yes	5
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Information Disclosure Statement (IDS) Form (SB08)		4	5	
	Transmittal Letter		1	3	
Warnings:					
Information:					
2	Foreign Reference	E-WO2013103782.pdf	3395927 fb512397c2b14b75e93a09dd1d8574a0cd1f98b3	no	45
Warnings:					
Information:					
3	Foreign Reference	F-WO2014031041.pdf	1434276 b0e915297b281b1f1c663906f928e77fb04181d8	no	50
Warnings:					
Information:					
4	Other Reference-Patent/App/Search documents	G-P-566702-EP-ESR-.pdf	35344 5463295bba2abf10ad9df6923f149dcc8ad6ae49	no	1
Warnings:					
Information:					
5	Other Reference-Patent/App/Search documents	H-P-566702-PC-IPRP-24OCT19.pdf	281838 b88354cdb9d8fa2c8c9b178434646a4a15092c59	no	6
Warnings:					
Information:					

6	Fee Worksheet (SB06)	fee-info.pdf	30512 78abd67eac2a8acfaf765173d018e47f60ff5b51	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	5250134	

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.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/603,252	10/07/2019	Yoseph KOREN	P-566702-US	6147

49443 7590 09/28/2020

Pearl Cohen Zedek Latzer Baratz LLP
1500 Broadway
12th Floor
New York, NY 10036

EXAMINER	
SHAMS, MOHAMMAD S	

ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
09/28/2020	ELECTRONIC

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

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

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

Arch-USPTO@PearlCohen.com
USPTO@PearlCohen.com

Office Action Summary	**Application No.** 16/603,252	**Applicant(s)** KOREN et al.	
	Examiner MOHAMMAD S SHAMS	**Art Unit** 2434	**AIA (FITF) Status** Yes

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

Period for Reply

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

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

Status

1)☑ Responsive to communication(s) filed on 10/07/2019.

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

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

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

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

Disposition of Claims*

5) ☑ Claim(s) 1-5,7-9,12-15,17-20,24 and 26-28 is/are pending in the application.

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

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-5,7-9,12-15,17-20,24 and 26-28 is/are rejected.

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

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

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

Application Papers

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

11)☑ The drawing(s) filed on 10/07/2019 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

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

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

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☑ All b)☐ Some** c)☐ None of the:

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

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

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

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

Attachment(s)

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

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date 10/07/2019.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-5, 7-9, 12-15, 17-20, 24, 26-28 are under examination.

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 Objections

2. **Claim 5 and 15** are objected to for reciting of limitation "HTTPS" and “IP” applicant fails to disclose the meaning of acronym HTTPS and IP and applicant's disclosure also fails to disclose the acronym definition. Appropriate correction is requested.

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(b):
(b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 4, 7, 17, 18, and 24 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out

and distinctly claim the subject matter which the inventor or a joint inventor (or for applications subject to pre-AIA 35 U.S.C. 112, the applicant), regards as the invention.

Claim 4 recites "data packet **repentance**." A claim limitation which is considered indefinite cannot be disregarded. It is unclear from the claim limitation how a data packet repentance would relate to the communication data pattern. Further, the specification fails to provide a reasonable means for repentance as it is related to a communicated data packet. As such, one of ordinary skill in the art would be unable to determine the scope of the claim language. Therefore, the claim is rejected for failing to specifically point out and distinctly claim the subject matter which the inventors regard as the invention. Examiner interprets a "data packet repentance" as a data packet that is an unwanted or threat data packet communication data for the purpose of the examination.

Claims 7, 17, 18, and 24 recite "determining, by the remote server, **the** communication data pattern of the at least one data packet", "**the** at least one data pattern compatible with the received request", "determining, by the remote server, **the** type of the at least one data packet", and "**the** response database" respectively. These recitations lack antecedent basis. Any claim not specifically addressed above is being rejected as incorporating the deficiencies of a claim upon which it depends. For the purpose of examination, the claims are being interpreted as reciting "a" instead of "the".

Claim Rejections - 35 USC § 103

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

The following is a quotation of 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.

The factual inquiries for establishing a background for determining obviousness under 35 U.S.C. 103 are summarized as follows:

1. Determining the scope and contents of the prior art.

2. Ascertaining the differences between the prior art and the claims at issue.

3. Resolving the level of ordinary skill in the pertinent art.

4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-5, 7-9, 12-15, 17-20, 24, and 26-28 are rejected under 35 U.S.C. 103 as being unpatentable over Moffat et al. (US PGPUB # 2013/0318347) in view of McGloin et al. (US PGPUB # 2012/0005720).

Regarding claim 1. Moffat does teach, a method of dynamic management of private data during communication between a remote server and a user's device, the method comprising **[Moffat, para. 0232, FIG. 1, user's computing device 101 is connected to the Internet, or to some other electronic, digital or analog, data-sharing network…]**:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request **[Moffat, para. 0232, 0250, FIG. 1, FIG. 4, the DSS server receives data transmitted by the user's computer 101, and responds to requests for data by sending, when appropriate, messages and/or data back to the user's computer 101 via the Internet 103. (Para. 0250), FIG. 4 illustrates the actions and events which are typical of a user's interaction with the private DSS specified in an embodiment. User interaction begins 401 following the initialization of the DSS client on the user's computing device 101. Following initialization, the DSS client program (i.e. the "DSS_CP") operating on the user's computing device mediates 404 the user's interaction with the DSS server(s) by responding 404 to his interactions 402 with the DSS_CP, as well as responds 404 to messages, requests and data received 410 from the DSS server(s).]**;

determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet **[Moffat, para. 0494, 0612, certain information will be**

made available to the DSS server regarding the various individual elements of user data. For example, in an embodiment, the DSS server stores and has access to the following information regarding each individual packet of data owned, authored, uploaded and/or associated with any particular user: (a) An identifier which uniquely identifies and distinguishes each data packet within the computers, servers and/or programs of the DSS server. (b) The media or data type, or category, of each data packet, e.g. original text, a comment on other media, photo, video, link, etc. (c) The relationship of each packet of data to any other packet(s) of data (if any), such as a comment related to some other piece of media. (d) The date and time at which each data packet, and/or the associated media stored therein, was created, uploaded, modified, etc. (Para. 0612) these heuristics might be based on characteristics related to a user's set of contacts, for instance, on the number, and/or geographical dispersion, of those contacts. They might be based on patterns of communication and sharing. For instance, if one user tends to disseminate relatively large numbers of images to his contacts, while not receiving many messages, or other types of media, in return, that might increase the likelihood of improper conduct. They might be based on the distribution of types of media in a user's account. For instance, if a user stores large numbers of images and videos, but very few status messages, then that might be suggestive of someone storing improper content. Many other potential heuristics are possible, and the uses of all such heuristics for the purpose of identifying abusive users are included within the scope of the possible embodiments.] ;

receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication **[Moffat, para. 0149, 0221, 0826, the system of 6 wherein the unencrypted data includes permission-related attributes specifying what operations a recipient is allowed, by the owner, creator or source of the information specified by unencrypted data, to perform on that copy of the original information concealed within the encrypted data packet, including, but not limited to permissions regarding the recipient's printing, saving to local storage, editing, saving to external storage (e.g. a USB drive, a writable DVD, etc.), etc., of the copy of the original information. (Para. 0221)the DSS server will also determine the relevance of each packet of user data with respect to the type of media, e.g. the media-specific "page" or "section" of the "user interface" being viewed by a user on his local computing device by means of his DSS client. The relevance of each packet of user data might include not only the type of media, but also its date of creation and/or uploading, e.g. more recent media is often deemed to be more relevant to a user. The relevance of a packet of user data might also be affected by whether or not it is related to some other piece of user data, such as a comment on a photo. The relevance of any particular packet of user data might also be related to other attributes of that packet of data, as well as other attributes, characteristics, or user preferences, related to the context established by the DSS client and the other packets of user data to be displayed. (Para. 0826), the data can be represented and manipulated as explained below. Potentially sensitive and/or embarrassing user data is encrypted with an**

encryption key known only to the user who generates the data and only to the DSS client's of the recipients authorized by the user to receive, read, view, hear and/or otherwise experience that data. Therefore, original user data (such as text, photos and/or videos) is encrypted and only these encrypted forms of user data are stored and transmitted by the private DSS. Only in the DSS client program of an authorized user of the DSS, i.e. one possessing the requisite decryption key, can encrypted user data be restored and experienced.];

Moffat does not explicitly teach, modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference.

However, McGloin does teach, modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference **[McGloin, para. 0003, 0025, FIG. 3, as a result, a user, such as a system designer, is informed when the comparison reveals that one or more of the privacy rules is violated. This information facilitates modification of the software application in order to comply with the privacy rules. (Para. 0025), FIG. 3 is a diagram showing one implementation of privacy rules engines in order to comply with applicable privacy rules. FIG. 3 shows two entities exchanging data from two different jurisdictions with each jurisdiction potentially having different privacy rules governing the import or export of data. Jurisdiction A (300) is shown with data privacy rules 310, such as laws, which govern the import and/or export of data from/to Jurisdiction A. Organization data assets and processes 320 are organizational assets with software applications (processes) that retrieve and**

store data. Privacy rules engine 330 is a rules engine that aids in privacy compliance when data is being sent from Jurisdiction A to Jurisdiction B 350 so that transmitted data 340 includes data types and formats that are determined by Jurisdiction A's privacy export rules and/or Jurisdiction B's privacy import rules. Data formats includes formatting data elements using encryption technology so that the privacy of certain data elements is maintained. Privacy rules compliant data 340 is transmitted to Jurisdiction B via computer network 200.]; and

Moffat further discloses, maintaining communication between the remote server and the user's device, with sharing of the modified data packets **[Moffat, para. 0436, 0558, if the user who generated the requested data packet has opted to have the DSS server maintain a log of all processing associated with that packet (such as by the DSS server and/or by any other user's DSS client) then, in response to the request for the packet's retrieval, the DSS server can generate a log record that captures data about the packet's sharing (e.g. noting for example, the identity of the user who has directly, or indirectly, made the request and subsequently received the packet, the time and date of the request, and so forth). The DSS server 2207 then saves this log entry 2210 in its associated storage device(s) 2212 and subsequently (likely upon request by the user) provides that log entry (and any other log entries) to the user whose data has been manipulated and/or otherwise processed. (Para. 0804), Each of the client programs and/or program configurations that the server is capable of sending to a user can be capable of: performing a unique set of functions, the availability or lack thereof being detectable by the server (for example, responding to a specific query from the**

server); providing a unique set of responses to a set of queries from the server; and executing a unique set of modifications to data packets transmitted from the client to the server; etc.].

Therefore, it would have been obvious to one of ordinary skilled in art before the effective filing date of claimed invention to modify the teachings of Moffat that provides and architecture for a data sharing system that facilitates the encryption, storage exchange and decryption of confidential and proprietary information (Please see abstract and para. 0022) with teachings of McGloin (McGloin, para. 0003, 0025, FIG. 3) that would enable Moffat while performing privacy action and modifying the data it would also provide an information feedback when user is attempting to send a data to a target location with the data element being in violation of privacy rules (McGloin, para. 0031).

Regarding claim 2. Moffat does teach, the method of claim 1, wherein the communication data type of the at least one data packet is determined from metadata of communication with the remote server **[Moffat, para. 0499, 0501, additional metadata would also be generated by the DSS, and stored locally on a user's computer by the DSS client, and/or stored within the DSS server. This metadata would be designed to provide the DSS with hints as to which other encrypted media elements are likely to be most relevant to a user's DSS client, with respect to any particular state of that DSS client. Some, or all, of such user data metadata might be encrypted and hidden from the DSS server if it would be deemed likely to contain user-related data, or if it might provide a risk to the security and/or privacy of user data. (Para. 0501), The generation and storage of such general and/or context-specific user data metadata can be particularly useful for**

embodiments in which only a minimal amount of information about the attributes of individual user data media elements is made available to the DSS server. When only a minimal amount of metadata, if any, is available to the DSS server to assist it in characterizing, sorting and prioritizing user data prior to its transmission to a DSS client, then metadata (especially metadata containing information related to relevance and priority of the media specified within the user data) would likely greatly improve the efficiency of future retrievals and/or transmissions of user data in response to requests by DSS clients.].

Regarding claim 3. Moffat does teach, the method of claim 1, further comprising:

determining, by the user's device, at least one communication data pattern of at least one data packet corresponding to the received request **[Moffat, para. 0611, heuristics based on attributes of each user's encrypted content, patterns of communication, network of contacts, and/or other factors discernable even in the absence of access to decrypted versions of the user data, will be used to identify those users most likely to be engaging in improper activities and/or to be storing and/or disseminating improper content; with the likelihood of random sampling of user data being at least partially influenced by the results of such analyses.]**; and

Moffat does not explicitly teach, modifying data packets corresponding to requests for sharing of responses corresponding to at least one data pattern, that are not compatible with the received privacy preference

However, McGloin does teach, modifying data packets corresponding to requests for sharing of responses corresponding to at least one data pattern, that are not compatible with the received privacy preference **[McGloin, para. 0025, FIG. 3 is a diagram showing one implementation of privacy rules engines in order to comply with applicable privacy rules. FIG. 3 shows two entities exchanging data from two different jurisdictions with each jurisdiction potentially having different privacy rules governing the import or export of data. Jurisdiction A (300) is shown with data privacy rules 310, such as laws, which govern the import and/or export of data from/to Jurisdiction A. Organization data assets and processes 320 are organizational assets with software applications (processes) that retrieve and store data. Privacy rules engine 330 is a rules engine that aids in privacy compliance when data is being sent from Jurisdiction A to Jurisdiction B 350 so that transmitted data 340 includes data types and formats that are determined by Jurisdiction A's privacy export rules and/or Jurisdiction B's privacy import rules. Data formats includes formatting data elements using encryption technology so that the privacy of certain data elements is maintained. Privacy rules compliant data 340 is transmitted to Jurisdiction B via computer network 200.]**,

Moffat further discloses: wherein the privacy preference comprises a list of allowed data patterns for sharing during communication **[Moffat, para. 0149, 0221, the system of 6 wherein the unencrypted data includes permission-related attributes specifying what operations a recipient is allowed, by the owner, creator or source of the information specified by unencrypted data, to perform on that copy of the original information concealed within the encrypted data packet, including, but**

not limited to permissions regarding the recipient's printing, saving to local storage, editing, saving to external storage (e.g. a USB drive, a writable DVD, etc.), etc., of the copy of the original information. (Para. 0221), the DSS server will also determine the relevance of each packet of user data with respect to the type of media, e.g. the media-specific "page" or "section" of the "user interface" being viewed by a user on his local computing device by means of his DSS client. The relevance of each packet of user data might include not only the type of media, but also its date of creation and/or uploading, e.g. more recent media is often deemed to be more relevant to a user. The relevance of a packet of user data might also be affected by whether or not it is related to some other piece of user data, such as a comment on a photo. The relevance of any particular packet of user data might also be related to other attributes of that packet of data, as well as other attributes, characteristics, or user preferences, related to the context established by the DSS client and the other packets of user data to be displayed.].

Therefore, it would have been obvious to one of ordinary skilled in art before the effective filing date of claimed invention to modify the teachings of Moffat that provides and architecture for a data sharing system that facilitates the encryption, storage exchange and decryption of confidential and proprietary information (Please see abstract and para. 0022) with teachings of McGloin (McGloin, para. 0003, 0025, FIG. 3) that would enable Moffat while performing privacy action and modifying the data it would also would provide an information feedback when user is attempting to send a data to a target location with the data element being in violation of privacy rules (McGloin, para. 0031).

Regarding claim 4. Moffat does teach, the method of claim 3 wherein the communication data pattern is determined based on a range selected from a group consisting of data packet frequency, data packet size, data packet speed, data packet count, data packet ratio compared to other data type flow, data packet repentance, and data packet order **[Moffat, para. 0122, The network of 1f in which some aspect of the sharing, including, but not limited to: the selection of data, products and/or services, the categories data, products and/or services, the quality data, products and/or services, the quantity of data, products and/or services, and/or the frequency of provision of data, products and/or services, may vary between a first and second other user. (Para. 0143), the system of 6 wherein the unencrypted data includes size of information specified by unencrypted data, e.g. original file size. (Para. 269), FIG. 7 is a simplified illustration of a basic data flow in a private DSS implemented in accordance with an embodiment herein. (Para. 0331), any attempt by the user 1301 to transmit a digital copy 1318 of the locally-stored copy of the document 1306 by means of some data distribution network 1319 (e.g. the Internet) to which his computing device 1302 is connected, to the computing device 1320 of some unauthorized recipient 1321, will only transmit the encrypted version of the document. (Para. 0334), the use of a private DSS of a type disclosed herein to control access to sensitive data within an organization benefits such organizations by making the copying and dissemination of sensitive data more difficult to perpetrate, more likely to be detected by others, more time-consuming and less likely to succeed.].**

Regarding claim 5. Moffat does teach, the method of claim 1, wherein the communication data type is determined based on data packet characteristics selected from a group consisting of data packet header, data packet footer, version number, IP address, HTTPS, file extension, encryption method, encoding method, keywords, driver, and communication protocol **[Moffat, para. 0425, 0612, 0622, another optional safeguard which may help to ensure the integrity of the log-in process is for a private DSS to require that the entire DSS client always be uploaded to a user's computing device, immediately following a successful log in, by means of an encrypted (e.g. an https) connection. (Para. 0612), if one user tends to disseminate relatively large numbers of images to his contacts, while not receiving many messages, or other types of media, in return, that might increase the likelihood of improper conduct. They might be based on the distribution of types of media in a user's account. For instance, if a user stores large numbers of images and videos, but very few status messages, then that might be suggestive of someone storing improper content. Many other potential heuristics are possible, and the uses of all such heuristics for the purpose of identifying abusive users are included within the scope of the possible embodiments. (Para. 0622), the efficiency with which they monetize their private DSS by targeting ads to users on the basis of the geographical location of the user. The DSS client and/or DSS server should be able to identify the approximate location of a user based on the IP address from which the client connects to the corresponding data-sharing network, browser attributes and/or other available attributes.]**.

Regarding claim 7. Moffat does teach, the method of claim 1, further comprising:

determining, by the remote server, the communication data pattern of the at least one data packet of the received request **[Moffat, para. 0275, The DSS client responds to any new requests by the user for access to contact data by requesting any available encrypted contact data from the DSS server. Upon receipt of that encrypted contact data, the DSS server uses the contact's decryption key (stored in the user's key locker) to decrypt the data. When contacts of the user create, upload and/or modify any of their data, the DSS server passes that encrypted user data to the user's DSS client. And, again, the DSS client retrieves the needed decryption key(s) from the user's key locker and decrypts the encrypted contact data.]**; and

linking at least one response from the user's device to a type of data packet from the user's device, wherein the linking is based on the communication data type and communication data pattern of the at least one response **[Moffat, para. 0341, FIG. 14B illustrates a method by which a DSS_CP can be loaded directly on to a user's computing device 1402. A browser program 1410 running on a user's computing device 1402 can connect to a DSS server 1409, through a data distribution network 1411 like the Internet, if the user enters the proper URL into the appropriate browser input. The DSS server can then return an installer program, or a link to such an installer program, which the user can choose to download. After the installer 1412 is downloaded, the user can execute that installer**

resulting in the installation of a "stand-alone" DSS_CP 1413 capable of running without a browser on the user's computing device 1402. Such a stand-alone DSS_CP can likely incorporate more functionality than a typical browser-based program and it can likely facilitate a user's utilization of a private DSS which used an uncommon, or poorly supported, data distribution network, e.g., a proprietary network based on the transmission and distribution of data through the electrical wiring of a house or other building.].

Regarding claim 8. Moffat does teach, the method of claim 1, further comprising:

identifying a response corresponding to a request for sharing of data packets, wherein the identified response is not compatible with the received privacy preference **[Moffat, para. 0257, 0609, FIG. 5, the request will typically be transmitted through the data sharing network 504, e.g. the Internet, by the network I/O subsystem 506 of the user's computing device 505. (Para. 0609), utilize tools within the DSS client to look for and detect improper content. This would eliminate the need for compromising the privacy of any user's data until, and unless, content which appears to be abusive is detected.]**; and

providing a response with at least one modified data packet corresponding to the request for sharing types of data packets **[Moffat, para. 0826, the data can be represented and manipulated as explained below. Potentially sensitive and/or embarrassing user data is encrypted with an encryption key known only to the user who generates the data and only to the DSS client's of the recipients**

authorized by the user to receive, read, view, hear and/or otherwise experience that data. Therefore, original user data (such as text, photos and/or videos) is encrypted and only these encrypted forms of user data are stored and transmitted by the private DSS. Only in the DSS client program of an authorized user of the DSS, i.e. one possessing the requisite decryption key, can encrypted user data be restored and experienced.].

Regarding claim 9. Moffat does teach, the method of claim 8, wherein the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption **[Moffat, para. 0559-0561, 0826. users are offered the ability to create and modify repositories of data dedicated to the maintenance of "to-do lists," accounting data (both personal and business), and other types of archives dedicated to special purposes, and/or special types of data, in which the user is able to vary the data through additions, deletions, edits and so forth. (Para. 0560), users are able to elect to have all, or some select portion, of the information which they generate or discover online automatically copied to one or more special-purpose personal archives. In an embodiment, these archives can be edited, and otherwise manipulated. This allows a user the ability to construct a variety of collections of information gathered, and/or in some other way generated, through online activity of some kind. (Para. 0561), for instance, a user searching for online tools which facilitate a**

user's creation of graphical illustrations might elect to collect those tools, or annotated links to the locations where such tools can be found, as well as samples of artwork which the user has created with the tools evaluated. The user might, at some point, elect to reorganize, and fully document, this collection so that it will be suitable for sharing with others. (Para. 826), certain information will be made available to the DSS server regarding the various individual elements of user data. For example, in an embodiment, the DSS server stores and has access to the following information regarding each individual packet of data owned, authored, uploaded and/or associated with any particular user: (a) An identifier which uniquely identifies and distinguishes each data packet within the computers, servers and/or programs of the DSS server. (b) The media or data type, or category, of each data packet, e.g. original text, a comment on other media, photo, video, link, etc. (c) The relationship of each packet of data to any other packet(s) of data (if any), such as a comment related to some other piece of media. (d) The date and time at which each data packet, and/or the associated media stored therein, was created, uploaded, modified, etc. (Para. 0558), users are offered a number of "dynamic personal archives" as well as the "static," "write-once" archives discussed earlier. These dynamic personal archives allow users to create collections of data in which they can modify the contents over time through deletions, edits, etc. These dynamic archives can be implemented such that the frequent modification of the contents is facilitated.].

Regarding claim 12. A method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request **[Moffat, para. 0232, 0250, FIG. 1, FIG. 4, the DSS server receives data transmitted by the user's computer 101, and responds to requests for data by sending, when appropriate, messages and/or data back to the user's computer 101 via the Internet 103. (Para. 0250), FIG. 4 illustrates the actions and events which are typical of a user's interaction with the private DSS specified in an embodiment. User interaction begins 401 following the initialization of the DSS client on the user's computing device 101. Following initialization, the DSS client program (i.e. the "DSS_CP") operating on the user's computing device mediates 404 the user's interaction with the DSS server(s) by responding 404 to his interactions 402 with the DSS_CP, as well as responds 404 to messages, requests and data received 410 from the DSS server(s).]**;

determining, by the remote server, at least one communication data pattern corresponding to the received request, wherein the at least one communication data pattern is determined in accordance with a behavior range of the communication data packet **[Moffat, para. 0601-0607, if a sample of a user's data appears to contain improper content, then the next step would be for the "examiner" (perhaps an automated system) to notify the respective user's DSS client. At that point, the DSS client would transmit additional elements of user PID (data) to the examiner to allow the examiner to either confirm, or rule out, the presence of abusive**

content, and/or the user's involvement in improper activities. (Para 0602), 1n an embodiment, if a user is deemed to have created, imported, stored, shared, etc., improper content within the private DSS, or if the user is deemed to be engaging in, or supporting (even passively), improper activities or behaviors, then the following steps (of an "abuse response protocol") will be executed: (Para. 0603), 1. The user's DSS client will be notified, and it will transmit to the examiner all of the user's encryption keys and decryption keys, including the decryption keys and usernames (and/or other account identifiers) of the user's contacts. (Para.0604) 2. An examiner will decrypt and examine the user data associated with the abusive user and each of his friends. (Para. 0605) 3. The examiner will make a final determination of whether or not the user is engaged in improper conduct and/or storing improper content. (Para. 0606) 4. The abusive user's data will be decrypted and copied to a separate storage location. And, a report will be filed with the appropriate legal authority(s). (Para. 0607) 5. The account of the abusive user will only be frozen, or otherwise limited, upon request by the appropriate legal authorities. This allows those authorities the opportunity to gather additional evidence, e.g. through sting operations, and to locate, and/or take into custody, the abusive user prior to warning being given to the abusive user.];

receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data patterns for sharing during communication **[Moffat, para. 0149, 0221, 0826, the system of 6 wherein the unencrypted data includes permission-related attributes specifying what**

operations a recipient is allowed, by the owner, creator or source of the information specified by unencrypted data, to perform on that copy of the original information concealed within the encrypted data packet, including, but not limited to permissions regarding the recipient's printing, saving to local storage, editing, saving to external storage (e.g. a USB drive, a writable DVD, etc.), etc., of the copy of the original information. (Para. 0221)the DSS server will also determine the relevance of each packet of user data with respect to the type of media, e.g. the media-specific "page" or "section" of the "user interface" being viewed by a user on his local computing device by means of his DSS client. The relevance of each packet of user data might include not only the type of media, but also its date of creation and/or uploading, e.g. more recent media is often deemed to be more relevant to a user. The relevance of a packet of user data might also be affected by whether or not it is related to some other piece of user data, such as a comment on a photo. The relevance of any particular packet of user data might also be related to other attributes of that packet of data, as well as other attributes, characteristics, or user preferences, related to the context established by the DSS client and the other packets of user data to be displayed. (Para. 0826), the data can be represented and manipulated as explained below. Potentially sensitive and/or embarrassing user data is encrypted with an encryption key known only to the user who generates the data and only to the DSS client's of the recipients authorized by the user to receive, read, view, hear and/or otherwise experience that data. Therefore, original user data (such as text, photos and/or videos) is encrypted and only these encrypted forms of user data

are stored and transmitted by the private DSS. Only in the DSS client program of an authorized user of the DSS, i.e. one possessing the requisite decryption key, can encrypted user data be restored and experienced];

Moffat does not explicitly teach, modifying data packets corresponding to requests for sharing of responses and corresponding data patterns that are not compatible with the received privacy preference.

McGloin does teach, modifying data packets corresponding to requests for sharing of responses and corresponding data patterns that are not compatible with the received privacy preference **[McGloin, para. 0003, 0025, As a result, a user, such as a system designer, is informed when the comparison reveals that one or more of the privacy rules is violated. This information facilitates modification of the software application in order to comply with the privacy rules. (Para. 0025), FIG. 3 is a diagram showing one implementation of privacy rules engines in order to comply with applicable privacy rules. FIG. 3 shows two entities exchanging data from two different jurisdictions with each jurisdiction potentially having different privacy rules governing the import or export of data. Jurisdiction A (300) is shown with data privacy rules 310, such as laws, which govern the import and/or export of data from/to Jurisdiction A. Organization data assets and processes 320 are organizational assets with software applications (processes) that retrieve and store data. Privacy rules engine 330 is a rules engine that aids in privacy compliance when data is being sent from Jurisdiction A to Jurisdiction B 350 so that transmitted data 340 includes data types and formats that are determined by Jurisdiction A's privacy export rules and/or Jurisdiction B's privacy import rules.**

Data formats includes formatting data elements using encryption technology so that the privacy of certain data elements is maintained. Privacy rules compliant data 340 is transmitted to Jurisdiction B via computer network 200.]; and

Moffat further discloses: maintaining communication between the remote server and the user's device, with sharing of the modified data packets **[Moffat, para. 0436, 0558, if the user who generated the requested data packet has opted to have the DSS server maintain a log of all processing associated with that packet (such as by the DSS server and/or by any other user's DSS client) then, in response to the request for the packet's retrieval, the DSS server can generate a log record that captures data about the packet's sharing (e.g. noting for example, the identity of the user who has directly, or indirectly, made the request and subsequently received the packet, the time and date of the request, and so forth). The DSS server 2207 then saves this log entry 2210 in its associated storage device(s) 2212 and subsequently (likely upon request by the user) provides that log entry (and any other log entries) to the user whose data has been manipulated and/or otherwise processed. (Para. 0804), Each of the client programs and/or program configurations that the server is capable of sending to a user can be capable of: performing a unique set of functions, the availability or lack thereof being detectable by the server (for example, responding to a specific query from the server); providing a unique set of responses to a set of queries from the server; and executing a unique set of modifications to data packets transmitted from the client to the server; etc.]**.

Therefore, it would have been obvious to one of ordinary skilled in art before the effective filing date of claimed invention to modify the teachings of Moffat that provides and architecture for a data sharing system that facilitates the encryption, storage exchange and decryption of confidential and proprietary information (Please see abstract and para. 0022) with teachings of McGloin (McGloin, para. 0003, 0025, FIG. 3) that would enable Moffat while performing privacy action and modifying the data it would also would provide an information feedback when user is attempting to send a data to a target location with the data element being in violation of privacy rules (McGloin, para. 0031).

Regarding method claim 13 that is same or similar to method claim 2 and similarly rejected.

Regarding claim 14. Moffat does teach, the method of claim 12, further comprising:

determining, by the remote server, the communication data type of the at least one data packet of the received request **[Moffat, para. certain information will be made available to the DSS server regarding the various individual elements of user data. For example, in an embodiment, the DSS server stores and has access to the following information regarding each individual packet of data owned, authored, uploaded and/or associated with any particular user: (a) An identifier which uniquely identifies and distinguishes each data packet within the computers, servers and/or programs of the DSS server. (b) The media or data**

type, or category, of each data packet, e.g. original text, a comment on other media, photo, video, link, etc. (c) The relationship of each packet of data to any other packet(s) of data (if any), such as a comment related to some other piece of media. (d) The date and time at which each data packet, and/or the associated media stored therein, was created, uploaded, modified, etc.]; and

modifying data packets corresponding to requests for sharing of responses and corresponding data patterns **[Moffat, para. 0274, After this process of initialization, the DSS client begins a cyclic pattern of interaction with the DSS server. The DSS client requests 711 from the DSS server 712 any encrypted data from the user and/or contacts appropriate to the context of the DSS client's user interface. Upon receipt of the encrypted user data 715, the DSS client uses the appropriate decryption key(s) to decrypt that data 716. The DSS client, for example, then makes this decrypted user data available to the user via the user interface.]**,

Moffat does not explicitly teach, corresponding to at least one communication data packet type, that are not compatible with the received privacy preference.

However, McGloin does teach, corresponding to at least one communication data packet type, that are not compatible with the received privacy preference **[McGloin, para. 0003, 0025, FIG. 3, as a result, a user, such as a system designer, is informed when the comparison reveals that one or more of the privacy rules is violated. This information facilitates modification of the software application in order to comply with the privacy rules. (Para. 0025), FIG. 3 is a diagram showing one implementation of privacy rules engines in order to comply with applicable privacy rules. FIG. 3 shows two entities exchanging data from two different**

jurisdictions with each jurisdiction potentially having different privacy rules governing the import or export of data. Jurisdiction A (300) is shown with data privacy rules 310, such as laws, which govern the import and/or export of data from/to Jurisdiction A. Organization data assets and processes 320 are organizational assets with software applications (processes) that retrieve and store data. Privacy rules engine 330 is a rules engine that aids in privacy compliance when data is being sent from Jurisdiction A to Jurisdiction B 350 so that transmitted data 340 includes data types and formats that are determined by Jurisdiction A's privacy export rules and/or Jurisdiction B's privacy import rules. Data formats includes formatting data elements using encryption technology so that the privacy of certain data elements is maintained. Privacy rules compliant data 340 is transmitted to Jurisdiction B via computer network 200.],

Moffat further does teach, wherein the privacy preference comprises a list of allowed data packet types for sharing during communication **[Moffat, para. 0149, 0221, 0826, the system of 6 wherein the unencrypted data includes permission-related attributes specifying what operations a recipient is allowed, by the owner, creator or source of the information specified by unencrypted data, to perform on that copy of the original information concealed within the encrypted data packet, including, but not limited to permissions regarding the recipient's printing, saving to local storage, editing, saving to external storage (e.g. a USB drive, a writable DVD, etc.), etc., of the copy of the original information. (Para. 0221)the DSS server will also determine the relevance of each packet of user data with respect to the type of media, e.g. the media-specific "page" or "section" of the "user**

interface" being viewed by a user on his local computing device by means of his DSS client. The relevance of each packet of user data might include not only the type of media, but also its date of creation and/or uploading, e.g. more recent media is often deemed to be more relevant to a user. The relevance of a packet of user data might also be affected by whether or not it is related to some other piece of user data, such as a comment on a photo. The relevance of any particular packet of user data might also be related to other attributes of that packet of data, as well as other attributes, characteristics, or user preferences, related to the context established by the DSS client and the other packets of user data to be displayed. (Para. 0826), the data can be represented and manipulated as explained below. Potentially sensitive and/or embarrassing user data is encrypted with an encryption key known only to the user who generates the data and only to the DSS client's of the recipients authorized by the user to receive, read, view, hear and/or otherwise experience that data. Therefore, original user data (such as text, photos and/or videos) is encrypted and only these encrypted forms of user data are stored and transmitted by the private DSS. Only in the DSS client program of an authorized user of the DSS, i.e. one possessing the requisite decryption key, can encrypted user data be restored and experienced.].

Therefore, it would have been obvious to one of ordinary skilled in art before the effective filing date of claimed invention to modify the teachings of Moffat that provides and architecture for a data sharing system that facilitates the encryption, storage exchange and decryption of confidential and proprietary information (Please see abstract and para. 0022) with teachings of McGloin (McGloin, para. 0003, 0025, FIG. 3)

that would enable Moffat while performing privacy action and modifying the data it would also would provide an information feedback when user is attempting to send a data to a target location with the data element being in violation of privacy rules (McGloin, para. 0031).

Regarding method claim 15 that is same or similar to method claim 5, and is similarly rejected.

Regarding claim 17. Moffat does teach, the method of claim 12, wherein the user's device is in communication with an external database with at least one communication data pattern corresponding to a request for sharing of data packets from the user's device, and wherein the at least one data pattern compatible with the received request is determined from the database **[Moffat, para. 0257, FIG. 5, The request will typically be transmitted through the data sharing network 504, e.g. the Internet, by the network I/O subsystem 506 of the user's computing device 505. After receiving the request for user data from the DSS_CP 509, the DSS system retrieves the user's encrypted data from storage 501, including but not limited to the user's encrypted key locker 502. And, after retrieving the encrypted key locker, the DSS system sends that encrypted file to the DSS_CP by means of the data sharing network 504.]**.

Regarding method claim 18 that is same or similar to method claim 7, and is similarly rejected.

Regarding method claim 19 that is same or similar to method claim 8, and is similarly rejected.

Regarding method claim 20 that is same or similar to method claim 9, and is similarly rejected.

Regarding claim 24. Moffat does teach, a system for dynamic management of private data during communication between a remote server and at least one user's device, the system comprising **[Moffat, para. 0232, FIG. 1, user's computing device 101 is connected to the Internet, or to some other electronic, digital or analog, data-sharing network…]**:

a communication data type database, comprising at least one communication data type corresponding to sharing of at least one data packet from the user's device **[Moffat, para. 0235, FIG. 2 illustrates a possible structure of a private DSS of a type of this disclosure. A group of users 201, 202, 203 creates accounts within the DSS 213. These users interact with the DSS 213 through local DSS client programs ("DSS_CP's") 205, 206, 207 running on their respective computing devices 208, 209, 210. These DSS_CP's utilize the hardware and software resources of the users' computing devices 208, 209, 210 to communicate with, and exchange data with, the DSS server(s) 204. The DSS_CP's 205, 206, 207 only transmit encrypted versions of any user data transmitted into the Internet or other data sharing network 211. And, only encrypted user data is received by the DSS server(s) 204 and/or stored on the storage device(s) of the DSS 212. The full central portion of an exemplary private DSS, i.e., the "DSS server" 213, includes,**

but is not limited to, some server(s) 204 and some storage device(s) and/or components 212.];

a privacy preference database, comprising a list of allowed types of data packets for sharing during communication with the at least one user's device **[Moffat, para. 0097, Disclosed herein is a method of sharing data between a source of data and one or more recipients (e.g. a person's "friends") in which the data may only be viewed, understood and/or modified by the source, or the recipients, of the data, which includes: (a) protecting the privacy of the data from viewing, disclosure and/or exploitation by other parties, including the owners and/or operators of the system facilitating such data sharing; and (b) wherein the protecting of the privacy of the data is by data obfuscation and/or encryption prior to its transmission from the computing device(s) of the source, and by the clarification and/or decryption of that obfuscated and/or encrypted data upon the computing devices of the recipients.]**;

a communication module, to allow communication between the remote server and the at least one user's device **[Moffat, para. 0232, FIG. 1 illustrates a possible connection scheme between the DSS client that a user would utilize in order to access a DSS and a server of the DSS. A user's computing device 101 is connected to the Internet, or to some other electronic, digital or analog, data-sharing network. A program on the user's computer 101 (e.g. a browser program, a "stand-alone" program, etc.) exchanges messages and data with a DSS server by sending 102 properly addressed messages and/or data into the network 103. Those user messages and/or data arrive, via the network 103 at a DSS server 105.**

The DSS server receives data transmitted by the user's computer 101, and responds to requests for data by sending, when appropriate, messages and/or data back to the user's computer 101 via the Internet 103.]; and

Moffat does not explicitly teach, a processor, coupled to the response database and to the privacy preference database, wherein the processor is configured to instruct the remote server to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of data packets for sharing

However, McGloin does teach, a processor, coupled to the response database and to the privacy preference database, wherein the processor is configured to instruct the remote server to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of data packets for sharing, **[McGloin, para. 0019, FIG.1, processors 110 coupled to processor interface bus 112. Processor interface bus 112 connects processors 110 to Northbridge 115, which is also known as the Memory Controller Hub (MCH). Northbridge 115 connects to system memory 120 and provides a means for processor(s) 110 to access the system memory. (Para. 0048), FIG. 11 is an exemplary flowchart diagram execution of the privacy rules engine to produce privacy compliant data. Processing commences at 1100 whereupon, at step 1110, the privacy rules engine receives request data 815, data type categorization 830 which was identified using the process shown in FIG. 9, and data flow categorization 850 which was identified using the process shown in FIG. 10. At step 1120 the first data element that is to be transmitted is selected. At step 1125, the privacy data type category of the selected data element is compared to the current data privacy rules stored in privacy rules data**

store 520. A decision is made as to whether a privacy rule matches the privacy data type category (decision 1130). If a privacy rule does not match the privacy data type category (e.g., no privacy rule applies to the selected data element's privacy data category), then decision 1130 branches to the "no" branch whereupon, at step 1140 the data element (raw data) is written to output transmission buffer 880 which stores privacy compliant data suitable for transmission to the target location.].

Moffat further discloses: and wherein the at least one data type is determined in accordance with characteristics of the communication data packet **[Moffat, para. , 0612, these heuristics might be based on characteristics related to a user's set of contacts, for instance, on the number, and/or geographical dispersion, of those contacts. They might be based on patterns of communication and sharing. For instance, if one user tends to disseminate relatively large numbers of images to his contacts, while not receiving many messages, or other types of media, in return, that might increase the likelihood of improper conduct. They might be based on the distribution of types of media in a user's account. For instance, if a user stores large numbers of images and videos, but very few status messages, then that might be suggestive of someone storing improper content. Many other potential heuristics are possible, and the uses of all such heuristics for the purpose of identifying abusive users are included within the scope of the possible embodiments.]**.

Therefore, it would have been obvious to one of ordinary skilled in art before the effective filing date of claimed invention to modify the teachings of Moffat that provides

and architecture for a data sharing system that facilitates the encryption, storage exchange and decryption of confidential and proprietary information (Please see abstract and para. 0022) with teachings of McGloin (McGloin, para. 0019, FIG. 1) that would enable Moffat while performing privacy action and modifying the data it would also would provide an information feedback when user is attempting to send a data to a target location with the data element being in violation of privacy rules (McGloin, para. 0031).

Regarding claim 26. Moffat does teach, the system of claim 24, McGloin further disclosese comprising a communication data pattern database, coupled to the processor and comprising at least one data pattern corresponding to sharing of at least one data packet from the user's device, wherein the processor is configured to modify data packets corresponding to requests for retrieval of data packets and communication data types that are not compatible with communication data patterns from a communication data pattern database **[McGloin, para. 0003, 0025, FIG. 3, as a result, a user, such as a system designer, is informed when the comparison reveals that one or more of the privacy rules is violated. This information facilitates modification of the software application in order to comply with the privacy rules. (Para. 0025), FIG. 3 is a diagram showing one implementation of privacy rules engines in order to comply with applicable privacy rules. FIG. 3 shows two entities exchanging data from two different jurisdictions with each jurisdiction potentially having different privacy rules governing the import or export of data. Jurisdiction A (300) is shown with data privacy rules 310, such as laws, which**

govern the import and/or export of data from/to Jurisdiction A. Organization data assets and processes 320 are organizational assets with software applications (processes) that retrieve and store data. Privacy rules engine 330 is a rules engine that aids in privacy compliance when data is being sent from Jurisdiction A to Jurisdiction B 350 so that transmitted data 340 includes data types and formats that are determined by Jurisdiction A's privacy export rules and/or Jurisdiction B's privacy import rules. Data formats includes formatting data elements using encryption technology so that the privacy of certain data elements is maintained. Privacy rules compliant data 340 is transmitted to Jurisdiction B via computer network 200.].

Therefore, it would have been obvious to one of ordinary skilled in art before the effective filing date of claimed invention to modify the teachings of Moffat that provides and architecture for a data sharing system that facilitates the encryption, storage exchange and decryption of confidential and proprietary information (Please see abstract and para. 0022) with teachings of McGloin (McGloin, para. 0019, FIG. 1) that would enable Moffat while performing privacy action and modifying the data it would also would provide an information feedback when user is attempting to send a data to a target location with the data element being in violation of privacy rules (McGloin, para. 0031).

Regarding claim 27. Moffat does teach, the system of claim 26, wherein data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor

data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory **[Moffat, para. 0235, FIG. 2 illustrates a possible structure of a private DSS of a type of this disclosure. A group of users 201, 202, 203 creates accounts within the DSS 213. These users interact with the DSS 213 through local DSS client programs ("DSS_CP's") 205, 206, 207 running on their respective computing devices 208, 209, 210. These DSS_CP's utilize the hardware and software resources of the users' computing devices 208, 209, 210 to communicate with, and exchange data with, the DSS server(s) 204. The DSS_CP's 205, 206, 207 only transmit encrypted versions of any user data transmitted into the Internet or other data sharing network 211. And, only encrypted user data is received by the DSS server(s) 204 and/or stored on the storage device(s) of the DSS 212. The full central portion of an exemplary private DSS, i.e., the "DSS server" 213, includes, but is not limited to, some server(s) 204 and some storage device(s) and/or components 212. (Para. 558), users are offered a number of "dynamic personal archives" as well as the "static," "write-once" archives discussed earlier. These dynamic personal archives allow users to create collections of data in which they can modify the contents over time through deletions, edits, etc. These dynamic archives can be implemented such that the frequent modification of the contents is facilitated. (Para. 0562), a user is able to change the attributes of one of his personal archives, for instance, changing a personal, private archive such as the one described above (dedicated to online tools for graphic illustrations) into a shared archive, either shared with a select group of other users or made public and accessible to any user. (Para.**

0565), such private shared archives might be used for many purposes. For instance, they might be used to compile historical, or chronological, data related to an activity, the evolution of a business, a topic of interest (such as hang gliding), etc. (Para. 0567), such private forums might be used to create online marketplaces where various goods are offered for sale, or purchased, by a select set of users who share a particular characteristic, e.g. an interest, a location, an employer, etc. For example, collectors of war-related postage stamps might organize a private forum wherein they could discuss stamps, and buy and sell their own stamps.].

Regarding claim 28. Moffat does teach, the system of claim 26, wherein at least the communication module and the processor are embedded on a single hardware component **[Moffat, para. 0232, FIG. 1 illustrates a possible connection scheme between the DSS client that a user would utilize in order to access a DSS and a server of the DSS. A user's computing device 101 is connected to the Internet, or to some other electronic, digital or analog, data-sharing network. A program on the user's computer 101 (e.g. a browser program, a "stand-alone" program, etc.)]**.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MOHAMMAD S SHAMS whose telephone number is (571)272-3406. The examiner can normally be reached on Monday-Friday 8:00 AM-5:30 PM.

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, Kambiz Zand can be reached on (571)272-3811. 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 https://ppair-my.uspto.gov/pair/PrivatePair. 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.

/MOHAMMAD S SHAMS/
Examiner, Art Unit 2434

/NOURA ZOUBAIR/
Primary Examiner, Art Unit 2434

Notice of References Cited	Application/Control No. 16/603,252	Applicant(s)/Patent Under Reexamination KOREN et al.	
	Examiner MOHAMMAD S SHAMS	Art Unit 2434	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-20180359811-A1	12-2018	Verzun; levgen	H04L63/0428	1/1
*	B	US-20140259147-A1	09-2014	L'Heureux; Israel	H04L63/083	726/14
*	C	US-20190149523-A1	05-2019	SHIN; Yoshihiro	G06F21/62	713/176
*	D	US-10348715-B2	07-2019	Ross; Brian G.	H04L63/0823	1/1
*	E	US-20170118638-A1	04-2017	Zhang; Qiang	H04L63/0876	1/1
*	F	US-10277614-B2	04-2019	Koide; Kazuhiro	H04L63/1408	1/1
*	G	US-20120005720-A1	01-2012	McGloin; Mark Alexander	G06F21/6263	726/1
	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

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

*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.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/603,252	KOREN et al.
	Examiner	Art Unit
	MOHAMMAD S SHAMS	2434

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

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

CLAIM		DATE								
Final	Original	09/19/2020								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	-								
	7	✓								
	8	✓								
	9	✓								
	10	-								
	11	-								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	-								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	-								
	22	-								
	23	-								
	24	✓								
	25	-								
	26	✓								
	27	✓								
	28	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	16/603,252	KOREN et al.
	Examiner	Art Unit
	MOHAMMAD S SHAMS	2434

CPC - Searched*		
Symbol	Date	Examiner
G06F21/6263, H04L63/0421, H04L63/0428	09/17/2020	M.S.S.

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
726	9	09/17/2020	

* 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
Applicant and Inventors Search	09/10/2020	M.S.S.
NPL, IP.com Search	09/17/2020	M.S.S.
EAST (Text and CPC) Search	09/22/2020	M.S.S.

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

/MOHAMMAD S SHAMS/ Examiner, Art Unit 2434	

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

BIB DATA SHEET

CONFIRMATION NO. 6147

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
16/603,252	10/07/2019 RULE	726	2434	P-566702-US

APPLICANTS
Privacy Rating Ltd., Ganey Tikva, ISRAEL

INVENTORS
Yoseph KOREN, Ganey Tikva, ISRAEL;
Yehonatan WASSERMAN, Kiryat Ono, ISRAEL;

**** CONTINUING DATA ***************************
This application is a 371 of PCT/IL2018/050359 03/28/2018

**** FOREIGN APPLICATIONS ***************************
ISRAEL 251683 04/09/2017

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
08/27/2020

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☑ Yes ☐ No	☑ Yes ☐ No	/MOHAMMAD S SHAMS/ Examiner's Signature	☐ Initials	ISRAEL	10	20	3

ADDRESS

Pearl Cohen Zedek Latzer Baratz LLP
1500 Broadway
12th Floor
New York, NY 10036
UNITED STATES

TITLE

SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

FILING FEE RECEIVED		
790	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	0	((("PRIVACY") near3 ("RATING") near3 ("LTD"))).AS,AANM.	USPAT	OR	ON	2020/09/10 17:21
S2	1	((("KOREN") near3 ("Yoseph"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/10 17:21
S3	1	((("WASSERMAN") near3 ("Yehonatan"))).INV.	US-PGPUB; USPAT; USOCR	OR	ON	2020/09/10 17:21
S4	2	dynamic near2 management near2 private near2 data	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/10 17:22
S6	58,795	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/10 17:28
S7	1	S2 and S6	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/10 17:35
S8	1	S6 and S3	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/10 17:36
S9	28	(("20190347442") or ("20190182903") or ("20170325286") or ("10708978") or ("10212761") or ("20190342749") or ("10278065") or ("20180049023") or ("20170187758") or ("20100274859") or ("9781170") or ("20170230427") or ("20170230426") or ("10051018") or ("20190034060") or ("20190034826") or	US-PGPUB; USPAT; USOCR; FPRS	OR	OFF	2020/09/12 16:34

		("20190075140") or ("20160119330") or ("20190036775")).PN.				
S10	23	(("9954907") or ("20100064307") or ("20170041381") or ("10567479") or ("9197600") or ("10467552") or ("20140259147") or ("20180359811") or ("20040042414") or ("20090147772") or ("20170180504") or ("20190238655") or ("20160105416") or ("10306009") or ("8613026") or ("20170359420") or ("20120290844")).PN.	US-PGPUB; USPAT; USOCR; FPRS	OR	OFF	2020/09/12 16:45
S11	26	(("10402580") or ("8804966") or ("20090080661") or ("20190280986") or ("20170257143") or ("20190319932") or ("20180241727") or ("20150100488") or ("20180198757") or ("10491575") or ("10397335") or ("20200067884") or ("8254582") or ("20160219024")).PN.	US-PGPUB; USPAT; USOCR; FPRS	OR	OFF	2020/09/12 16:46
S12	77	S9 S10 S11	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/12 16:46
S15	2	"20130318347"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/12 16:59
S16	6	(("20090150968") or ("20070172066") or ("20100095119") or ("20040010467") or ("20100031335") or ("20100046749")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2020/09/12 17:08
S19	7	"2013318347"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2020/09/17 14:04
S20	2	"20130318347"	US-PGPUB; USPAT; USOCR; FPRS	OR	ON	2020/09/17 14:04
S21	1	"20190149523"	US-PGPUB; USPAT; USOCR;	OR	ON	2020/09/17 15:23

			FPRS; EPO			
S22	10	"10348715"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/17 15:24
S23	6	"20170118638"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/17 15:28
S34	0	"16603252"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/18 09:31
S35	3	"10277614"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/18 10:27
S36	6	"20170118638"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/19 07:49
S37	3	"20150180839"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/19 07:50
S38	4	"20170054674"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/19 07:51
S39	2	"20160323305"	US-PGPUB; USPAT; USOCR;	OR	ON	2020/09/21 11:04

			FPRS; EPO			
S40	0	(request$3 ask$3 seek$3 requir$3 solicit$3) with (shar$3 exchang$3 communicat$3 exchang$3) and (compatiblity agreeable matched incompatible acceptable) same (privacy secrecy privateness confidentiality) near5 (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:35
S41	322,293	(request$3 ask$3 seek$3 requir$3 solicit$3) with (shar$3 exchang$3 communicat$3 exchang$3) and (compatiblity agreeable matched incompatible acceptable)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:36
S42	77	S41 and (privacy secrecy privateness confidentiality) near5 (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:37
S43	58,877	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:38
S44	588	"L1" and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:38
S45	27	S42 and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 15:39
S46	4	"20020015422"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:09
S47	4	"20140119380"	US-PGPUB; USPAT; USOCR;	OR	ON	2020/09/21 16:13

			FPRS; EPO			
S48	44	S42 and ((characteristics traits identify$3 attributes pattern) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:19
S49	39	S41 and (privacy secrecy privateness confidentiality) near5 (data near2 packet) same (shar$3 exchang$3 communicat$3 exchang$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:48
S50	2	S49 and (modify$3 alter$3 revis$3 adjust$3 amend$3 modulat$3 chang$3) near5 (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 16:51
S51	12	S42 and ((modificat$3 chang$3 alter$3 revis$3 adjust$3 amend$3) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 21:21
S56	0	S41 and ((modificat$3 chang$3 alter$3 revis$3 adjust$3 amend$3) with (data near2 packet)) same ((incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 21:58
S57	0	S41 and (privacy secrecy privateness confidentiality) near5 (data near2 packet) same (incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:01
S58	0	S44 and (privacy secrecy privateness confidentiality) near5 (data near2 packet) same (incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:01
S59	31	S44 and (incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security)	US-PGPUB; USPAT; USOCR;	OR	ON	2020/09/21 22:02

			FPRS; EPO			
S60	3,093	S41 and (incompatible contridictory clash$3 unfit$3 disagreeabble mismatched compatible) with (privacy security)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:10
S61	475	S60 and S43	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:10
S62	6	S61 and (privacy secrecy privateness confidentiality) near5 (data near2 packet)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/21 22:12
S63	3,911	((outgoing transmit$4 send$3) with (data packet information)) same (privacy near4 (set$4 policy rule))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:25
S64	468	((outgoing transmit$4 send$3) with (data packet information)) same (privacy near4 (set$4 policy rule)) with (complian$2 comply$3 complies violat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:27
S65	1,516	((outgoing transmit$4 send$3) with (data packet information)) same ((privacy security) near4 (set$4 policy rule)) with (complian$2 comply$3 complies violat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:28
S66	58,901	(G06F21/6263 H04L63/0421 H04L63/0428).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 12:29
S67	88	S65 and S66	US-PGPUB; USPAT; USOCR;	OR	ON	2020/09/22 12:29

			FPRS; EPO			
S68	5	S67 and ((modificat$3 chang$3 alter$3 revis$3 adjust$3 amend$3) with (data near2 packet))	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 13:54
S69	6	"20120005720"	US-PGPUB; USPAT; USOCR; FPRS; EPO	OR	ON	2020/09/22 15:01

EAST Search History (Interference)

<This search history is empty>

9/22/2020 9:57:54 PM
C:\Users\mshams\Documents\EAST\Workspaces\16603252.wsp

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. 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.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	1	of	2

Complete if Known	
Application Number	Not yet assigned
Filing Date	Herewith
First Named Inventor	Yoseph KOREN
Art Unit	Not yet assigned
Examiner Name	Not yet assigned
Attorney Docket Number	P-566702-US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A	US-2013/318347	11-28-2013	MOFFAT BRIAN LEE	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
						☐
						☐
						☐
						☐
						☐
						☐
						☐
						☐

Examiner Signature	/MOHAMMAD S SHAMS/	Date Considered	09/12/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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 2 hours 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, 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 (1-800-786-9199) and select option 2.

7 October 2019

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.S.S./

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. 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.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	Not yet assigned
Filing Date	Herewith
First Named Inventor	Yoseph KOREN
Art Unit	Not yet assigned
Examiner Name	Not yet assigned
Attorney Docket Number	P-566702-US

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (where appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	B	Internatioanl Search Report of PCT Application No. PCT/IL2018/050359 mailed on July 12, 2018	☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐

Examiner Signature	/MOHAMMAD S SHAMS/	Date Considered	09/12/2020

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

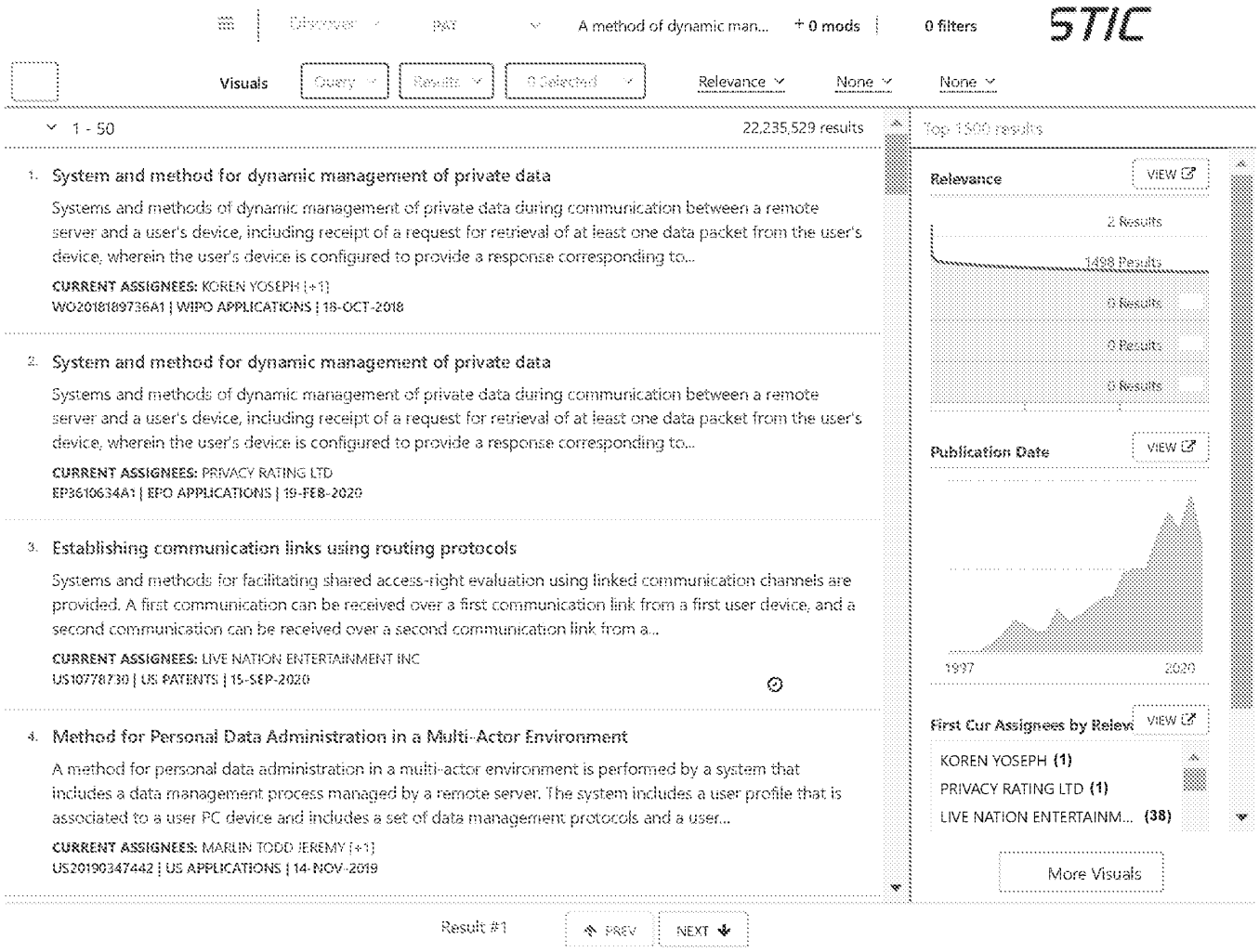
[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 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 2 hours 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, 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 (1-800-786-9199) and select option 2.

7 October 2019

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /M.S.S./


Discover
PAT
A method of dynamic man...
+ 0 mods
0 filters
STIC
Visuals
Query
Results
0 Selected
Relevance
None
None
1 - 50
22,235,529 results
Top 1500 results
1. System and method for dynamic management of private data
Systems and methods of dynamic management of private data during communication between a remote server and a user's device, including receipt of a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to...
CURRENT ASSIGNEES: KOREN YOSEPH [+1]
WO2018189736A1 | WIPO APPLICATIONS | 18-OCT-2018
2. System and method for dynamic management of private data
Systems and methods of dynamic management of private data during communication between a remote server and a user's device, including receipt of a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to...
CURRENT ASSIGNEES: PRIVACY RATING LTD
EP3610634A1 | EPO APPLICATIONS | 19-FEB-2020
3. Establishing communication links using routing protocols
Systems and methods for facilitating shared access-right evaluation using linked communication channels are provided. A first communication can be received over a first communication link from a first user device, and a second communication can be received over a second communication link from a...
CURRENT ASSIGNEES: LIVE NATION ENTERTAINMENT INC
US10778730 | US PATENTS | 15-SEP-2020
4. Method for Personal Data Administration in a Multi-Actor Environment
A method for personal data administration in a multi-actor environment is performed by a system that includes a data management process managed by a remote server. The system includes a user profile that is associated to a user PC device and includes a set of data management protocols and a user...
CURRENT ASSIGNEES: MARLIN TODD JEREMY [+1]
US20190347442 | US APPLICATIONS | 14-NOV-2019
Relevance
VIEW
2 Results
1498 Results
0 Results
0 Results
0 Results
Publication Date
VIEW
1997
2020
First Cur Assignees by Relev
VIEW
KOREN YOSEPH (1)
PRIVACY RATING LTD (1)
LIVE NATION ENTERTAINM... (38)
More Visuals
Result #1
PREV
NEXT

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 16/603,252

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	150		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	260		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	380		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 50 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 230 =	0.00			
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).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	790		TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	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.

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET

Substitute for Form PTO-1360
(For use with Form PTO/SB/06)

Application Number	Filing Date
16603252	

Applicant(s) Yoseph KOREN

* May be used for additional claims or amendments

CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT	
	Indep	Depend	Indep	Depend	Indep	Depend
1	1		1			
2		1		1		
3		1		1		
4		1		1		
5		1		1		
6		1	---	---		
7		1		1		
8		1		1		
9		1		1		
10		1	---	---		
11		1	---	---		
12	1		1			
13		1		1		
14		1		1		
15		1		1		
16		1	---	---		
17		1		1		
18		1		1		
19		1		1		
20		1		1		
21		1	---	---		
22		1	---	---		
23		1	---	---		
24	1		1			
25		1	---	---		
26		1		1		
27		1		1		
28		1		1		
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						
Total Indep	3		3		0	
Total Depend	25	↵	17	↵	0	↵
Total Claims	28		20		0	

	*		*		*	
	Indep	Depend	Indep	Depend	Indep	Depend
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						

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

U.S. APPLICATION NO.	FIRST NAMED INVENTOR	ATTY. DOCKET NO.
16/603,252	Yoseph KOREN	P-566702-US

49443
Pearl Cohen Zedek Latzer Baratz LLP
1500 Broadway
12th Floor
New York, NY 10036

INTERNATIONAL APPLICATION NO.	
PCT/IL2018/050359	
I.A. FILING DATE	PRIORITY DATE
03/28/2018	04/09/2017

CONFIRMATION NO. 6147
371 ACCEPTANCE LETTER

OC000000119541556

Date Mailed: 08/31/2020

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office, in its capacity as a Designated / Elected Office (37 CFR 1.495), has ACCEPTED the above identified international application for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above. A Filing Receipt will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE "FILING DATE or 371(c) DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1) and (c)(2) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN BELOW.** The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363)

10/07/2019
DATE OF RECEIPT OF 35 U.S.C.
371(c)(1) and (c)(2) REQUIREMENTS

The following items have been received:

- Indication of Small Entity Status
- Copy of the International Application filed on 10/07/2019
- Copy of the International Search Report filed on 10/07/2019
- Preliminary Amendments filed on 10/07/2019
- Information Disclosure Statements filed on 10/07/2019
- Inventor's Oath or Declaration filed on 10/07/2019
- Request for Immediate Examination filed on 10/07/2019
- U.S. Basic National Fees filed on 10/07/2019
- Assignment filed on 10/07/2019
- Assignee Statement for PGPUB filed on 10/07/2019
- Authorize Access to Search Results filed on 10/07/2019
- Priority Documents filed on 10/07/2019
- Power of Attorney filed on 10/07/2019
- Authorization to Permit Access filed on 10/07/2019
- Application Data Sheet (37 CFR 1.76) filed on 10/07/2019

FORM PCT/DO/EO/903 (371 Acceptance Notice)

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

LESLIE R CHASE

Telephone: (703) 756-1026

FORM PCT/DO/EO/903 (371 Acceptance Notice)

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 NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
16/603,252	10/07/2019		790	P-566702-US	20	3

CONFIRMATION NO. 6147

49443
Pearl Cohen Zedek Latzer Baratz LLP
1500 Broadway
12th Floor
New York, NY 10036

FILING RECEIPT



Date Mailed: 08/31/2020

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)

Yoseph KOREN, Ganey Tikva, ISRAEL;
Yehonatan WASSERMAN, Kiryat Ono, ISRAEL;

Applicant(s)

Privacy Rating Ltd., Ganey Tikva, ISRAEL

Assignment For Published Patent Application

Privacy Rating Ltd., Ganey Tikva, ISRAEL

Power of Attorney: The patent practitioners associated with Customer Number 49443

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/IL2018/050359 03/28/2018

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)
ISRAEL 251683 04/09/2017

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: 08/27/2020

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/603,252**

Projected Publication Date: 12/10/2020

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **
Title

SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

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 AssetsControl, 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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/603,252		Yoseph KOREN	P-566702-US	6147

49443 7590 11/15/2019

Pearl Cohen Zedek Latzer Baratz LLP
1500 Broadway
12th Floor
New York, NY 10036

EXAMINER	
ART UNIT	PAPER NUMBER

NOTIFICATION DATE	DELIVERY MODE
11/15/2019	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):

Arch-USPTO@PearlCohen.com
USPTO@PearlCohen.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Application of
KOREN, YOSEPH, et al.
Application No.: 16/603,252
Filed: 07 October 2019
Attorney Docket No.: P-566702-US
For: SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

: DECISION ON REQUEST TO
: PARTICIPATE IN THE PATENT
: PROSECUTION HIGHWAY
: PROGRAM AND PETITION
: TO MAKE SPECIAL UNDER
: 37 CFR 1.102(a)

This is a decision on the request to participate in the Patent Prosecution Highway (PPH) program and the petition under 37 CFR 1.102(a), filed October 07, 2019, to make the above-identified application special.

The request and petition are **GRANTED**.

DISCUSSION

A grantable request to participate in the PPH pilot program and petition to make special require:

1. The U.S. application for which participation in the Global/IP5 PPH pilot program is requested must have the same earliest date, whether this is the priority date or filing date, as that of a corresponding national or regional application filed with another Global/IP5 PPH participating office or a corresponding PCT international application for which one of the Global/IP5 PPH participating offices was the International Searching Authority (ISA) or the International Preliminary Examining Authority (IPEA).

2. Applicant must:

    a. Ensure all the claims in the U.S. application must sufficiently correspond or be amended to sufficiently correspond to the allowable/patentable claim(s) in the corresponding Office of Earlier Examination (OEE) application and
    b. Submit a claims correspondence table in English;

3. Examination of the U.S. application has not begun;

4. Applicant must submit:

a. Documentation of prior office action:
   i. a copy of the office action(s) just prior to the "Decision to Grant a Patent" from each of the Global/IP5 PPH participating office application(s) containing the allowable/patentable claim(s) or
   ii. if the allowable/patentable claims(s) are from a "Notification of Reasons for Refusal" then the Notification of Reasons for Refusal or
   iii. if the Global/IP5 PPH participating office application is a first action allowance then no office action from the Global/IP5 PPH participating office is necessary should be indicated on the request/petition form or
   iv. the latest work product in the international phase of the OEE PCT application;

b. An English language translation of the Global/IP5 PPH participating office action or work product from (4)(a)(i)-(ii) or (iv) above;

5. Applicant must submit:

   a. An IDS listing the documents cited by the Global/IP5 PPH participating office examiner in the Global/IP5 PPH participating office action or work product (unless already submitted in this application);
   b. Copies of the documents except U.S. patents or U.S. patent application publications (unless already submitted in this application).

The request to participate in the PPH pilot program and petition comply with the above requirements. Accordingly, the above-identified application has been accorded "special" status.

Telephone inquiries concerning this decision should be directed to Dale Hall at (571)272-3586.

All other inquiries concerning the examination or status of the application is accessible in the PAIR system at http://portal.uspto.gov.

This application will be forwarded to the examiner for action on the merits commensurate with this decision once this application's formality reviews have been completed.

/Dale A. Hall/
Paralegal Specialist, OPET

CLAIMS

1. A method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request;

determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request;

receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication;

modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference; and

maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

2. The method of claim 1, wherein the communication data type of the at least one data packet is determined from metadata of communication with the remote server.

3. The method of claim 1, further comprising:

determining, by the user's device, at least one communication data pattern of at least one data packet corresponding to the received request; and

modifying data packets corresponding to requests for sharing of responses corresponding to at least one data pattern, that are not compatible with the received privacy preference,

wherein the privacy preference comprises a list of allowed data patterns for sharing during communication.

4. The method of claim 1, wherein the communication data pattern is determined based on a range selected from a group consisting of: data packet frequency, data packet size, data packet speed, data packet count, data packet ratio compared to other data type flow, data packet repentance, and data packet order.

5. The method of claim 1, wherein the communication data type is determined based on data packet characteristics selected from a group consisting of: data packet header, data packet footer, version number, IP address, HTTPS, file extension, encryption method, encoding method, keywords, driver, and communication protocol.

6. The method of claim 1, wherein the user's device is in communication with an external database with at least one data packet type corresponding to a request for sharing of data packets from the user's device, and wherein the type of data packets is determined from the database.

7. The method of claim 1, further comprising:

determining, by the remote server, the communication data pattern of the at least one data packet of the received request; and

linking at least one response from the user's device to a type of data packet from the user's device, wherein the linking is based on the communication data type and communication data pattern of the at least one response.

8. The method of claim 1, further comprising:

identifying a response corresponding to a request for sharing of data packets, wherein the identified response is not compatible with the received privacy preference; and

providing a response with at least one modified data packet corresponding to the request for sharing types of data packets.

9. The method of claim 8, wherein the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

10. The method of claim 1, further comprising:

identifying a communication pattern between the server and the user's device, wherein the communication pattern comprises at least one request for retrieval of at least one data packet from the user's device and corresponding responses; and

issuing an alert upon detection of a change in the identified communication pattern.

11. The method of claim 1, wherein data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

12. A method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request;

determining, by the remote server, at least one communication data pattern corresponding to the received request;

receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data patterns for sharing during communication;

modifying data packets corresponding to requests for sharing of responses and corresponding data patterns that are not compatible with the received privacy preference; and

maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

13. The method of claim 12, wherein the communication data pattern of the at least one response is determined from metadata of communication with the remote server.

14. The method of claim 12, further comprising:

determining, by the remote server, the communication data type of the at least one data packet of the received request; and

modifying data packets corresponding to requests for sharing of responses and corresponding data patterns, corresponding to at least one communication data packet type, that are not compatible with the received privacy preference,

wherein the privacy preference comprises a list of allowed data packet types for sharing during communication.

15. The method of claim 12, wherein the communication data type is determined based on data packet characteristics selected from a group consisting of: data packet header, data packet footer, version number, IP address, HTTPS, file extension, encryption method, encoding method, keywords, driver, and communication protocol.

16. The method of claim 12, wherein the communication data pattern is determined based on a range selected from a group consisting of: data packet frequency, data packet size, data packet speed, data packet count, data packet ratio compared to other data type flow, data packet repentance, and data packet order.

17. The method of claim 12, wherein the user's device is in communication with an external database with at least one communication data pattern corresponding to a request for sharing of data packets from the user's device, and wherein the at least one data pattern compatible with the received request is determined from the database.

18. The method of claim 12, further comprising:

determining, by the remote server, the type of the at least one data packet of the received request; and

linking at least one data pattern to a type of data packet from the user's device, wherein the linking is based on the communication data type and the communication data pattern of the at least one response.

19. The method of claim 12, further comprising:

identifying a communication data pattern corresponding to a request for sharing of data packet types, wherein the identified data pattern is not compatible with the received privacy preference; and

providing a response with at least one modified data packet corresponding to the request for sharing types of data packets.

20. The method of claim 19, wherein the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

21. The method of claim 12, further comprising issuing an alert upon detection of a request for sharing data packets, wherein the detected request does not correspond to at least one of communication data type and communication data pattern that is compatible with the received privacy preference.

22. The method of claim 12, further comprising:

identifying a communication pattern between the server and the user's device, wherein the communication pattern comprises at least one request for retrieval of at least one data packet from the user's device and corresponding responses; and

issuing an alert upon detection of a change in the identified communication pattern.

23. The method of claim 12, wherein data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

24. A system for dynamic management of private data during communication between a remote server and at least one user's device, the system comprising:

a communication data type database, comprising at least one communication data type corresponding to sharing of at least one data packet from the user's device;

a privacy preference database, comprising a list of allowed types of data packets for sharing during communication with the at least one user's device;

a communication module, to allow communication between the remote server and the at least one user's device; and

a processor, coupled to the response database and to the privacy preference database,

wherein the processor is configured to instruct the remote server to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of data packets for sharing.

25. The system of claim 24, further comprising a user interface to issue an alert upon detection of a request for retrieval of data packets that is not compatible with the privacy preference.

26. The system of claim 24, further comprising a communication data pattern database, coupled to the processor and comprising at least one data pattern corresponding to sharing of at least one data packet from the user's device, wherein the processor is configured to modify data packets corresponding to requests for retrieval of data packets and communication data types that are not compatible with communication data patterns from a communication data pattern database.

27. The system of claim 26, wherein data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

28. The system of claim 26, wherein at least the communication module and the processor are embedded on a single hardware component.

SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

FIELD OF THE INVENTION

[001] The present invention relates to data management. More particularly, the present invention relates to systems and methods for dynamic management of private data.

BACKGROUND OF THE INVENTION

[002] During communication with external remote servers different types of data are automatically (and uncontrollably) shared, sometimes without the knowledge of the user (e.g., the owner of the data). There are currently only limited ways for the user to manage which data should be shared, with which parties, and at what time periods and/or under what circumstances such that privacy agreements cannot be fully enforced. For example, securing private elements of a user's device engaging in a transaction with a service provider, has been a challenge for many years with the rapid development of computer technology.

[003] In recent years, an increasing number of communication sessions are being biased (in terms of shared data and application usage) toward one party which is advantageous due to technological superiority, formal regulation power, and/or any other item. Such biasing may occur due to rapid development of communication related software, as well as due to development of computer technology.

[004] Social network service providers usually collect user (private) data, for example collect user's online habits. Data collection is usually carried out by a service provider requesting to share user's (private) information while the user's device automatically shares the requested information accordingly. Actions are executed by dedicated software (e.g., social plug in), which upload data requests when visiting web sites and/or applications. Such requests may be direct script by the service provider (e.g. cookie etc.), or indirect script hidden within links to other (partner) application provider (e.g. social plug-in, SDK, API etc.). While some devices allow blocking collection of certain private parameters, for example the location, only data emerging from sensors, such as global positioning system (GPS) sensors, can be managed by user while other sources of location (e.g. mobile network, IP provider, country, time zone) cannot be controlled so that in that case location information can still be collected. Thus, location information can be collected

while bypassing the instructions of the user (e.g., collecting location from cellular carrier data). Other examples from the same nature may include retrieving form data, retrieving data from flash memory and several other items which do not have the full (or partial) ability to disable and/or block data collection. Some service providers can also collect user data in order to transfer and/or sell to third parties (e.g., to present dedicated ads in the future). Another example may be avoiding biased exchange of information both from the user and the service provider perspectives.

SUMMARY OF THE INVENTION

[005] There is thus provided, in accordance with some embodiments of the invention, a method of dynamic management of private data during communication between a remote server and a user's device, the method including receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request, determining, by the user's device, the data type of the at least one data packet corresponding to the received request, receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference includes a list of allowed data packet types for sharing during communication, modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference, and maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

[006] In some embodiments, the type of the at least one data packet may be determined from metadata of communication with the remote server. In some embodiments, the method further includes determining, by the user's device, pattern of at least one response corresponding to the received request, and modifying data packets corresponding to requests for sharing of responses, corresponding to at least one data pattern, that are not compatible with the received privacy preference, wherein the privacy preference includes a list of allowed data patterns for sharing during communication. In some embodiments, the user's device includes a database with at least one data packet type corresponding to a request for sharing of data packets from the user's device, and wherein the type of data packets is determined from the database.

[007] In some embodiments, the method further includes linking at least one response to a type of data packet from the user's device, wherein the linking is based on the type and pattern of the at least one response. In some embodiments, the method further includes identifying a response corresponding to a request for sharing of data packets, wherein the identified response is not compatible with the received privacy preference, and providing a response with at least one modified data packet corresponding to the request for sharing types of data packets. In some embodiments, the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

[008] In some embodiments, the method further includes identifying a communication pattern between the server and the user's device, wherein the communication pattern includes at least one request for retrieval of at least one data packet from the user's device and corresponding responses, and issuing an alert upon detection of a change in the identified communication pattern.

[009] In some embodiments, data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

[010] There is thus provided, in accordance with some embodiments of the invention, a method of dynamic management of private data during communication between a remote server and a user's device, the method including receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request, determining, by the user's device, at least one data pattern corresponding to the received request, receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference includes a list of allowed data patterns for sharing during communication, modifying data packets corresponding to requests for sharing of responses and corresponding data patterns that are not compatible with the received privacy preference, and maintaining communication between the remote server and the user's device, with sharing of the modified responses.

[011] In some embodiments, the pattern of the at least one response is determined from metadata of communication with the remote server. In some embodiments, the method further includes determining, by the user's device, the type of the at least one data packet of the received request, and modifying data packets corresponding to requests for sharing of responses and corresponding data patterns, corresponding to at least one data packet type, that are not compatible with the received privacy preference, wherein the privacy preference includes a list of allowed data packet types for sharing during communication.

[012] In some embodiments, the user's device includes a database with at least one data pattern corresponding to a request for sharing of data packets from the user's device, and wherein the at least one data pattern compatible with the received request is determined from the database. In some embodiments, the method further includes determining, by the user's device, the type of the at least one data packet of the received request, and linking at least one data pattern to a type of data packet from the user's device, wherein the linking is based on the pattern of the at least one response.

[013] In some embodiments, the method further includes identifying a data pattern corresponding to a request for sharing of data packet types, wherein the identified data pattern is not compatible with the received privacy preference, and providing a response with at least one modified data packet corresponding to the request for sharing types of data packets. In some embodiments, the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

[014] In some embodiments, the method further includes issuing an alert upon detection of a request for sharing data packets, wherein the detected request does not correspond to at least one of data type and data pattern that is compatible with the received privacy preference. In some embodiments, the method further includes identifying a communication pattern between the server and the user's device, wherein the communication pattern includes at least one request for retrieval of at least one data packet from the user's device and corresponding responses, and issuing an alert upon detection of a change in the identified communication pattern.

[015] In some embodiments, data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect

attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

[016] There is thus provided, in accordance with some embodiments of the invention, a system for dynamic management of private data during communication between a remote server and at least one user's device, the system including a data type database, including at least one data type corresponding to sharing of at least one data packet from the user's device, a privacy preference database, including a list of allowed types of data packets for sharing during communication with the at least one user's device, a communication module, to allow communication between the remote server and the at least one user's device, and a processor, coupled to the response database and to the privacy preference database, wherein the processor is configured to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of data packets for sharing.

[017] In some embodiments, the system further includes a user interface to issue an alert upon detection of a request for retrieval of data packets that is not compatible with the privacy preference. In some embodiments, the system further includes a data pattern database, coupled to the processor, wherein the processor is configured to modify data packets corresponding to requests for retrieval of data packets and data types that are not compatible with data patterns from a data pattern database.

[018] In some embodiments, data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory. In some embodiments, at least the communication module and the processor are embedded on a single hardware component.

BRIEF DESCRIPTION OF THE DRAWINGS

[019] The subject matter regarded as the invention is particularly pointed out and distinctly claimed in the concluding portion of the specification. The invention, however, both as to organization and method of operation, together with objects, features, and advantages thereof, may best be understood by reference to the following detailed description when read with the accompanying drawings in which:

[020] Fig. 1 shows a schematic block diagram of an exemplary computing device, according to some embodiments of the invention;

[021] Fig. 2 schematically illustrates a data mapping system, according to some embodiments of the invention;

[022] Fig. 3A schematically illustrates examplary mapping of data type database, according to some embodiments of the invention;

[023] Fig. 3B schematically illustrates examplary mapping of data pattern database, according to some embodiments of the invention;

[024] Fig. 3C schematically illustrates examplary mapping of privacy preference table, according to some embodiments of the invention;

[025] Fig. 4 schematically illustrates a data management system, according to some embodiments of the invention;

[026] Fig. 5 shows a flowchart for a method of management of data packets with a sharing algorithm during communication between a remote server and a user's device, according to some embodiments of the invention;

[027] Figs. 6A-6B show flowcharts for a method of dynamic management of private data during communication between a remote server and a user's device, according to some embodiments of the invention; and

[028] Fig. 7 schematically illustrates a data management system 700 for dynamic management of private data that is embedded on a hardware component, according to some embodiments of the invention.

[029] It will be appreciated that for simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference numerals may be repeated among the figures to indicate corresponding or analogous elements.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[030] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will be understood by those skilled in the art that the present invention may be practiced without these specific

details. In other instances, well-known methods, procedures, and components have not been described in detail so as not to obscure the present invention.

[031] Although embodiments of the invention are not limited in this regard, discussions utilizing terms such as, for example, "processing," "computing," "calculating," "determining," "establishing", "analyzing", "checking", or the like, may refer to operation(s) and/or process(es) of a computer, a computing platform, a computing system, or other electronic computing device, that manipulates and/or transforms data represented as physical (e.g., electronic) quantities within the computer's registers and/or memories into other data similarly represented as physical quantities within the computer's registers and/or memories or other information non-transitory storage medium that may store instructions to perform operations and/or processes. Although embodiments of the invention are not limited in this regard, the terms "plurality" and "a plurality" as used herein may include, for example, "multiple" or "two or more". The terms "plurality" or "a plurality" may be used throughout the specification to describe two or more components, devices, elements, units, parameters, or the like. Unless explicitly stated, the method embodiments described herein are not constrained to a particular order or sequence. Additionally, some of the described method embodiments or elements thereof can occur or be performed simultaneously, at the same point in time, or concurrently.

[032] Reference is made to Fig. 1, showing a schematic block diagram of an exemplary computing device, according to embodiments of the present invention. Computing device 100 may include a controller 105 that may be, for example, a central processing unit processor (CPU), special purpose processor such as a graphic processing unit (GPU), communication control processing (CCP), a chip or any suitable computing or computational device, an operating system 115, a memory 120, a storage 130, an input devices 135 and an output device 140. Controller 105 may be configured to carry out methods as disclosed herein by for example executing code or software.

[033] Operating system 115 may be or may include any code segment designed and/or configured to perform tasks involving coordination, scheduling, arbitration, supervising, controlling or otherwise managing operation of computing device 100, for example, scheduling execution of programs. Operating system 115 may be a commercial operating system. Memory 120 may be or may include, for example, a Random Access Memory (RAM), a read only memory (ROM), a Dynamic RAM (DRAM), a Synchronous DRAM

(SD-RAM), a double data rate (DDR) memory chip, a Flash memory, a volatile memory, a non-volatile memory, a cache memory, a buffer, a short term memory unit, a long term memory unit, or other suitable memory units or storage units. Memory 120 may be or may include a plurality of, possibly different memory units.

[034] Executable code 125 may be any executable code, e.g., an application, a program, a process, automated task, software bots configured to manage data communication and user data collection (e.g., botnet), software adapted to perform artificial intelligence (AI), e.g. machine learning, deep learning, task or script. Executable code 125 may be executed by controller 105 possibly under control of operating system 115. Where applicable, executable code 125 may carry out operations described herein in real-time. Computing device 100 and executable code 125 may be configured to update, process and/or act upon information at the same rate the information, or a relevant event, are received. In some embodiments, more than one computing device 100 may be used. For example, a plurality of computing devices (in serial and/or parallel) that include components similar to those included in computing device 100 may be connected to a network and used as a system.

[035] Storage 130 may be or may include, for example, a hard disk drive, a universal serial bus (USB) device or other suitable removable and/or fixed storage unit. Content may be stored in storage 130 and may be loaded from storage 130 into memory 120 and may be stored in read only memory (ROM) to be loaded into memory 120 where it may be processed by controller 105. In some embodiments, some of the components shown in Fig. 1 may be omitted. For example, memory 120 may be a non-volatile memory having the storage capacity of storage 130. Accordingly, although shown as a separate component, storage 130 may be embedded or included in memory 120.

[036] Input devices 135 may be or may include a mouse, a keyboard, a touch screen or pad or any suitable input device. In some embodiments, computing device 100 receives input from a sensor such as global positioning system (GPS), camera, microphone, accelerometer, light sensor, compass, and any other sensor. It will be recognized that any suitable number of input devices may be operatively connected to computing device 100 as shown by block 135. Output devices 140 may include one or more displays, indicators, speakers, haptic output and/or any other suitable output devices. It will be recognized that any suitable number of output devices may be operatively connected to computing device 100 as shown by block 140. Any applicable input/output (I/O) devices may be connected

to computing device 100 as shown by blocks 135 and 140. For example, a wired or wireless network interface card (NIC), a modem, a universal serial bus (USB) device or external hard drive, cellular network connection, optical network connection, Bluetooth, and NFC may be included in input devices 135 and/or output devices 140.

[037] Embodiments of the invention may include an article such as a computer or processor non-transitory readable medium, or a computer or processor non-transitory storage medium, such as for example a memory, a disk drive, or a USB flash memory, encoding, including or storing instructions, e.g., computer-executable instructions, which, when executed by a processor or controller, carry out methods disclosed herein. For example, a storage medium such as memory 120, computer-executable instructions such as executable code 125 and a controller such as controller 105.

[038] Some embodiments may be provided in a computer program product that may include a non-transitory machine-readable medium, with instructions stored thereon, which may be used to program a computer, or other programmable devices, to perform methods as disclosed herein. Embodiments of the invention may include an article such as a computer or processor non-transitory readable medium, or a computer or processor non-transitory storage medium, such as for example a memory, a disk drive, or a USB flash memory, encoding, including or storing instructions, e.g., computer-executable instructions, which when executed by a processor or controller, carry out methods disclosed herein. The storage medium may include, but is not limited to, any type of disk including magneto-optical disks, semiconductor devices such as read-only memories (ROMs), random access memories (RAMs), such as a dynamic RAM (DRAM), erasable programmable read-only memories (EPROMs), flash memories, electrically erasable programmable read-only memories (EEPROMs), magnetic or optical cards, or any type of media suitable for storing electronic instructions, including programmable storage devices.

[039] A system according to embodiments of the invention may include components such as, but not limited to, a plurality of central processing units (CPU) or any other suitable multi-purpose or specific processors or controllers, a plurality of input units, a plurality of output units, a plurality of memory units, and a plurality of storage units. A system may additionally include other suitable hardware components and/or software components. In some embodiments, a system may include or may be, for example, a personal computer, a desktop computer, a mobile computer, a laptop computer, a notebook computer, a

terminal, a workstation, a server computer, a Personal Digital Assistant (PDA) device, a tablet computer, a network device, a smartphone, IOT device, action specific computerized machine (such as a dedicated robot) or any other suitable computing device. Unless explicitly stated, the method embodiments described herein are not constrained to a particular order or sequence. Additionally, some of the described method embodiments or elements thereof can occur or be performed at the same point in time.

[040] Reference is now made to Fig. 2, which schematically illustrates a data mapping system 200 for mapping of private data during communication with a remote server 201, according to some embodiments of the invention. The direction of arrows in Fig. 2 may indicate the direction of information flow. In order to manage private data for individual users, data mapping system 200 may initially map data types and data patterns (for example as a calibration process), as further described hereinafter. It should be noted that private data as used hereinafter may refer to any data and/or portion of data representing user's behavior, habits, characteristics, opinions, preferences, tendencies, relations, actions, status parameters (e.g., social, health, economic/wealth, legal, dependencies, being part of group and the like) and the like. In some embodiments, the user may be a computerized device (e.g., IOT, bot and the like) automatically operating on the user's behalf, so that the private data may refer to data and/or characteristics of the computerized device. Private data may also include privacy data and/or privacy preference(s).

[041] A user may choose based on private preference to share some private data and not to share other private data. Users may choose to share same private data with specific server and/or application and not to share it with different servers and/or application. In some embodiments, users may change such preference(s) at any applicable point in time. In some embodiments, private data may be automatically created to represent at least one feature of a computerized device and/or of the user of the computerized device. In some embodiments, private data may include at least one communication pattern and/or communication origin and destination and/or digital footprint and/or digital trace and/or digital response and/or digital reference. In some embodiments, private data may be received from analysis of data and/or from an external sensor and/or other source.

[042] The server 201 may be coupled to processor 202 such as controller 105, shown in Fig. 1. In some embodiments, processor 202 may receive at least one data packet 203 from server 201 to be mapped. For instance, processor 202 may receive at least one data packet

203 from a set of predetermined (or pre-classified) data packets 203. In some embodiments, processor 202 may receive from server 201 a request for sharing at least one data packet 203, for instance a request to share data packet with a contact name or contact directory data, where an automatic response may be created for each such request. It should be noted that data of such responses may also be considered as data packets 203 (e.g., to be mapped).

[043] In some embodiments, data mapping system 200 may include at least one data type database 204 and/or at least one data pattern database 205 and/or at least one privacy preference database 206 coupled to processor 202. In some embodiments, processor 202 may analyze the received data packet 203 to determine data type 207 of the data packet 203, for example by verifying at least one characteristic of the data packet 203. An examplary mapping of data types 207 is shown in Fig. 3A.

[044] In some embodiments, processor 202 may receive (e.g., from a user) privacy preference 209 to map the privacy preference database 206 for each data type and/or data pattern of the at least one data packet 203. In some embodiments, data mapping system 200 may include a modification algorithm 210, coupled to processor 202, and configured to, modify content of data packets according to at least one privacy preference 209 (e.g., nullify a content of a data packet). For example, the user may select a privacy preference 209 for forbidden sharing of location such that modification algorithm 210 may modify the content of the data packet 203 per a predetermined algorithm, for instance randomly modify the location (country) to any other country from a list of countries (e.g., Italy).

[045] Reference is now made to Fig. 3A, which schematically illustrates examplary mapping of data type database 204, according to some embodiments of the invention. Processor 202 may receive a request to share at least one data packet 203 (e.g., from server 201) and analyze characteristics of the at least one data packet 203, for example analyze characteristics of automatically created responses for the request. In some embodiments, the content of the received at least one data packet 203 may be analyzed for purposes of data type mapping.

[046] According to some embodiments, characteristics of the received at least one data packet 203 may be determined and dynamically fitted to an 'i'-dimensional vector 304 (e.g., static characteristics determined from metadata). It should be noted that while the characteristics vector 304 shown in Fig. 3A is five-dimensional, such vectors may have a

large number of characteristics. For example, an injective vector having dimensions of 50 characteristics (so that 'i'=50) or more. In some embodiments, an increased number of parameters in the characteristics vector 304 may improve chances of correctly determining the data type 207 until optimal determination of various data types may be achieved.

[047] At least one of the following characteristics of a data packet 203 may be injectively determined for each data packet: header, footer, version number, request by hostname/IP, sent to hostname/IP, server hostname/IP, IP address, file extension, , standard title, non-standard title, , encryption yes/no, encryption method, encoding yes/no, encoding method (e.g., 'UTF8'), whole file, chunked file, keywords, API version, SDK version, Social plug-in version, driver, communication protocol, action verbs, HTTP/HTTPS, URL Part Names, and/or any other specific character 'i' within the at least one data packet 203. The determined characteristics vector 304 may be associated with a particular data type 207 (since every data packet 203 corresponds to some data type 207), that may be still unknown (e.g., in terms of its content) and for instance indicated as data type 'j'. In some embodiments, processor 202 may receive at least one pre-classified data packet 203 with a known data type. In some embodiments, the data type 207 of characteristics vector 304 for the data-mapping stage, may be determined by reading the content of the corresponding data packet 203, for example reading content for the country name, web browsing history, operating system, etc.

[048] Such data types 207 (or characteristics vectors 304) that are gathered by processor 202, and possibly still having unknown data type content (e.g., data type 'j') at this stage, may be stored (e.g., stored in memory such as memory 120 shown in Fig. 1) at data type database 204 in order to carry out the data type mapping. Processor 202 may map the stored data types to link characteristics vectors 304 with data types 207. In some embodiments, processor 202 may determine that characteristics vectors 304 having at least one identical characteristic may correspond to a particular data type 207 (e.g. Web content search history type).

[049] Reference is now made back to Fig. 2. In some embodiments, data pattern database 205 may include at least one data pattern 208 corresponding to responses to sharing of at least one data packet 203. Similarly to mapping of data types (e.g., as shown in Fig. 3A), processor 202 may map data patterns of responses to request of sharing data packets 203. It should be noted that while the data type 207 of a data packet 203 may correspond to

static parameters (e.g., email address), the data patterns 208 may correspond to features of the dynamic data flow of data packet 203 that may be regarded as the "behavior" of the data packet 203.

[050] Reference is now made to Fig. 3B, which schematically illustrates examplary mapping of data pattern database 205, according to some embodiments of the invention. Processor 202 may receive at least one data packet 203 (e.g., from server 201), for example at least one response (or data packet) corresponding to a request for sharing the data packet 203 to analyze pattern behavior of the at least one response (or data packet). In some embodiments, the content of the received at least one data packet 203 may be analyzed to determine the data pattern. For example, at least one response may injectively correspond to a request for sharing at least one data packet 203 and/or a characteristic of the data packet 203 (e.g., a picture file from memory or from camera).

[051] It should be noted that while the pattern vector 305 shown in Fig. 3B is four-dimensional, such vectors may have a large number of features or ranges. For example, an injective vector 305 having dimensions of 100 features and/or ranges (so that 'm'=100) or more. At least one of the following dynamic features of a data pattern may be determined for each data packet: frequency (e.g., appearance(s) per second), size (e.g., in kilobytes), speed (in kilobytes per second), count (e.g., numbers), ratio (e.g., compared to other datatype flow), repeat (e.g., cyclic order), order, server reference (e.g., website reference such as "example.com/feature") and/or any combination thereof and/or other pattern behavior 'm' within the at least one data packet. In some embodiments, ranges for every feature (e.g., frequency) may be determined (e.g., lowest and highest frequency) as a feature of the data pattern 208. In some embodiments, a range may refer to non-discrete values (in contrast to discrete or static values in data type mapping, as shown in Fig. 3A), for instance a range defining number of website sub references (e.g., "example.com/sub-feature/sub-feature" with two sub references).

[052] The determined feature or pattern behavior vector 305 may be associated with a particular data pattern 208 (since every data packet 203 corresponds to some data pattern 208), that may be still unknown and for instance indicated as data pattern 208 'n'. In some embodiments, processor 202 may receive at least one pre-classified data packet 203 with a known data pattern.

[053] Such data patterns 208 that are gathered by processor 202, and possibly still having unknown data pattern 'n' at this stage, may be stored (e.g., stored in memory such as memory 120 shown in Fig. 1) at data pattern database 205 in order to carry out the data pattern mapping. Processor 202 may map the stored data patterns 'n' to link behavior vectors 305 with data patterns 208. In some embodiments, processor 202 may determine that pattern behavior vectors 305 having at least one identical characteristic and/or range may correspond to a data pattern 208 (e.g., same frequency range). In some embodiments, data patterns 208 may be determined according to logical conditions and/or ranges, for example for responses having frequency and size features in within predetermined thresholds.

[054] Reference is now made to Fig. 3C, which schematically illustrates examplary mapping of privacy preference table 306, according to some embodiments of the invention. Processor 202 may receive at least one data packet 203 (e.g., from server 201), for example at least one response (or data packet) corresponding to a request for sharing the data packet 203 to analyze type and pattern behavior of the at least one response (or data packet) to create data type database 204 and data pattern database 205 as described above. In some embodiments, processor 202 may receive (e.g., from a user) privacy preference database 206 to map the privacy preference table 306 for each data type (content) and/or data pattern of the at least one data packet 203. For example, the user may fill a privacy preference template (e.g., selecting to allow sharing of username) for different options of data types and/or data patterns to determine the privacy preference table 306. In case that some data packet is forbidden for sharing (e.g., contact data and/or a password), the content of that data packet may be, for example randomly, modified by predetermined modification algorithm 210 such that the modified content (e.g., nullified password or randomly replaced to a dummy contact name from a list) may be shared. In some embodiments, processor 202 may only check the data type such that no pattern is checked in order to determine the policy to apply, for example sharing of password data types may be completely forbidden so that data patterns are not checked. In some embodiments, processor 202 may detect an IoT device and only check the data pattern where the data type may not be checked. In some embodiments, processor 202 may only check the data pattern such that no data type is checked, for example checking frequency limit and modifying in accordance with the predefined limitations. In some embodiments,

repetition in at least one forbidden characteristic (e.g., forbidden frequency) may cause blocking of data sharing.

[055] Reference is now made back to Fig. 2. In some embodiments, privacy preference database 206 may include at least one privacy preference 209 such as a template to link privacy preferences for the determined data types 207 and/or data patterns 208 and/or modification algorithm 210. For example, privacy preference database 206 may include an un-populated matrix with data types 207 and/or data patterns 208 and/or modification algorithm 210 such that a user may choose which data types (content) 207 and/or data patterns 208 to share. In some embodiments, data mapping system 200 may include a modification algorithm 210, coupled to processor 202, and configured to manage sharing of at least one data packet 203 based on its data type 207 and/or data pattern 208 to comply with at least one privacy preference 209. The operation of the modification algorithm 210 is further described in Fig. 5, hereinafter.

[056] In some embodiments, data mapping system 200 (shown in Fig. 2) may be used as a system to determine collection of uncontrolled information from hardware equipment. Some manufacturers embed into their products, hidden agent(s) which transmits at least one hidden data packet. As may be apparent to one of ordinary skill in the art, such systems and methods may identify "back door" ability which may be part of the hardware core functionality and/or part of unit's embedded software. In some embodiments, by implementing the data mapping system 200 (shown in Fig. 2), unrecognized type and/or pattern of data packet may be determined, wherein the unrecognized type and/or pattern of data packet may be generated internally (in contrast to being requested by the server). Such data packet may be stored and further investigated for its origin and destination.

[057] Reference is now made to Fig. 4, which schematically illustrates a data management system 400 for dynamic management of private data during communication between a remote server 401 (such as server 201 in Fig. 2) and at least one user's device 411, according to some embodiments of the invention. The direction of arrows in Fig. 4 may indicate the direction of information flow. It should be noted that the at least one user's device 411 may be a computerized device such as computing device 100, shown in Fig. 1.

[058] In some embodiments, data management system 400 may include a data type database 404 (such as data type database 204 in Fig. 2), coupled to processor 402, such

that processor 402 may modify data packets (e.g., modify responses) to requests for retrieval of data packets 403 that are not compatible with data types from a data type database 404 and/or with data patterns from a data pattern database 405. In some embodiments, data management system 400 may further include a user interface 413 to issue an alert upon detection of a request for retrieval of data packets 403 that is not compatible with the privacy preference. In some embodiments, data packets 403 from the user's device 411 may be a response created as full or partial extraction(s) selected from the group consisting of any one of user's device files (permanent or temporary), user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory user's device static memory or the like.

[059] In some embodiments, data management system 400 may further include a user database 421 and/or a server database 431 for mapping of users and/or servers. Each user and/or user's device 411 using data management system 400 may be registered in user database 421 with corresponding privacy preference from privacy preference database 406, such that each user and/or user's device 411 may be linked to at least one privacy preference from privacy preference database 406. In some embodiments, server database 431 may include a list of servers 401 for communication with user devices 411. For example, a user may determine a predefine list of servers 401 for sharing of data (e.g., determine a whitelist). Thus, privacy preference database 406 may link privacy and/or sharing preferences for each user and/or server and/or data type and/or data pattern.

[060] In some embodiments, data management system 400 may perform at least one of sharing, blocking and/or modifying, per the modification algorithm 410 (e.g., such as modification algorithm 210, shown in Fig. 2), data packets 403 during communication between server 401 and user's device 411 according to the corresponding privacy preference from privacy preference database 406. For example, requests for sharing of data packets 403 of unrecognized data type may be blocked, requests for sharing of data packets 403 of allowed data type are shared, and requests for sharing of data packets 403 of forbidden data type are modified such that a predetermined response may be shared (e.g., nullify of contact data and randomly change to different mobile carrier from carrier list). In some embodiments, modification algorithm 410 may be configured for each mapped data type and/or data pattern so as to maintain communication as well as the

privacy preference by, for example randomly, modifying forbidden data packet (content) for sharing.

[061] In some embodiments, data mapping system 200 (shown in Fig. 2) may be continuously updates such that blocked unrecognized data types may be stored in a dedicated memory (such as memory 120 in Fig. 1) until this data type is mapped and recognized.

[062] In some embodiments, data management system 400 may perform at least one of sharing, blocking and modifying data packets 403 during communication between server 401 and user's device 411 in substantially real time such that the user may continue operation of user's device 411 while data management system 400 may operate in the background and/or operate in application mode for some operating systems (e.g., IOS) and/or some browsers (e.g., Safari). In some embodiments, data management system 400 (in contrast to the data-mapping stage) may handle encrypted data packets 403 since determination of data type does not read and concern the actual content of the data packet 403 even if the content is encrypted. It should be noted that while the mapping stage (e.g., described in Figs. 2 and 3A-3C) may require reading the content of the data packets for initial determination of data type and/or data pattern and/or privacy preference, the data management system 400, in contrast, does not need to read the actual content of the data packets.

[063] In some embodiments, data management system 400 may include a data pattern database 405 (such as data pattern database 205 in Fig. 2) with at least one data pattern corresponding to sharing of at least one data packet 403 (such as data packet 203 in Fig. 2) from user's device 411. In some embodiments, various data packets may be analyzed (e.g., by a processor) to determine reoccurring data patterns and thereby create data pattern database 405. As may be apparent to one of ordinary skill in the art, computerized devices such as user's device 411 may include a plurality of data packets 403 with various information (e.g., time zone, type of operating system, location, web browsing history, mouse movement, external audio, eye's focus tracking etc.) regarding the user's device 411.

[064] During communication with remote servers such as server 401, the server may send requests for sharing of these data packets 403, wherein the user's device 411 may automatically provide a corresponding response (or data packet) that is compatible with

the received request without knowledge, control and/or authorization of the user. According to some embodiments, data management system 400 may manage data packets 403 that are shared with server 401 according to a predefined privacy preference. In some embodiments, data management system 400 may further include a privacy preference database 406 (such as privacy preference database 206 in Fig. 2) with a predetermined privacy preference and/or a list of allowed and/or forbidden types of data packets 403 for sharing and/or modifying and/or, if not recognized, for blocking during communication with the at least one user's device 411. In some embodiments, at least some elements of the data management system 400 may be similar to corresponding elements in data mapping system 200, for example privacy preference database 406 while the content of data packet is not read.

[065] In some embodiments, data management system 400 may further include a communication module 412 configured to allow communication between the server 401 and the at least one user's device 411. In some embodiments, a user may determine at least one privacy preference from privacy preference database 406 with privacy preferences for data types and/or data patterns that the user allows for sharing (and/or forbidden types to be modified and/or, if not recognized types, to be blocked), for example the user may choose to block sharing of location data of any kind.

[066] In some embodiments, data management system 400 may further include a processor 402 (such as controller 105, shown in Fig. 1) coupled to the data pattern database 405 and to the privacy preference database 406. In some embodiments, processor 402 may be coupled to communication module 412. In some embodiments, processor 402 may be embedded in user's device 411. In some embodiments, processor 402 may determine at least one data pattern for sharing of data packet 403 that is for example compatible with the list of allowed types of data packets 403 from data type database 404 for sharing. In some embodiments, processor 402 may be embedded in server 401.

[067] In some embodiments, data management system 400 may operate in user's device 411 (e.g., in the form of internal proxy) to manage sharing of data packets 403, while data management system 400 may not affect other functionalities of the user's device 411 so as to allow uninterrupted usage of the device.

[068] Reference is now made to Fig. 5, which shows a flowchart for a method of management of data packets with a sharing algorithm during communication between a

remote server and a user's device, according to some embodiments of the invention. The processor (e.g., processor 402) may provide a data packet 403, for instance in response to a request for sharing of data. The received data packet 403 may be checked 501 for known or unknown element, for instance checked 501 for known data type and/or known data pattern based on data type database 404 and/or data pattern database 405. According to some embodiments, unknown elements may be determined as unrecognized and be blocked 510 by the sharing algorithm and not shared (e.g., with the server).

[069] In some embodiments, known elements may be checked 502 for allowed or forbidden elements, for instance checked 502 for allowed data type and/or allowed data pattern based on privacy preference database 406. According to some embodiments, allowed elements may be shared 520 by the sharing algorithm. According to some embodiments, forbidden elements may be, for example randomly, modified 530 by the predetermined modification algorithm 410 with sharing 520 of the modified content (e.g., with the server). For example, a user choosing not to share the country name may choose a privacy preference to modify such data packet to always share a random country name from a list of countries (e.g., "France") by modifying the data packet to be shared with the user, in order to maintain ongoing communication with the server.

[070] It should be noted that with data management system 400, the user may choose features for sharing such that other features that are forbidden for sharing may be modified so as to allow continuous and uninterrupted communication with the server.

[071] Reference is now made to Fig. 6A, which shows a flowchart for a method of dynamic management of private data during communication between a remote server 401 and a user's device 411, according to some embodiments of the invention. In some embodiments, user's device 411 may receive 601 a request for retrieval of at least one data packet 403 from the user's device 411, wherein the user's device 411 may provide a response corresponding to the received request.

[072] In some embodiments, the user's device 411 may determine 602 the data type of the at least one data packet 403 corresponding to the received request. In some embodiments, the user's device 411 may receive 603 a privacy preference for the user's device 411, wherein the privacy preference includes a list of allowed (or forbidden) data packet types for sharing (or randomly modifying per the predetermined modification algorithm for each forbidden data type) during communication. In some embodiments,

data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference may be modified 604. In some embodiments, responses to requests for sharing of data packets 403 of unrecognized type may be blocked. In some embodiments, communication between the remote server 401 and the user's device 411 may be maintained 605 with sharing of the modified data packets (e.g., responses).

[073] In some embodiments, the user's device 411 may determine a pattern of at least one response corresponding to the received request, and modify data packets (e.g., responses) to requests for sharing of data packets 403 corresponding to at least one data pattern that are not compatible with the received privacy preference. In some embodiments, the privacy preference may include a list of allowed data patterns for sharing during communication.

[074] It should be noted that such predetermined modification per each forbidden data packet type, may be a fixed or random action, depend on the user's preference and the content (e.g. nullify for password and randomly change to different country from countries list). For data packets that are not compatible with the received privacy preference (as determined by the user) may allow users to optimally control sharing of their data. For example, a user choosing not to share location data may use the system to randomly modify the data packets during communication (as above) such that the location data may not be transferred via other means (e.g., user's instruction not to share location, application blocking only sensor GPS data while sharing country code data).

[075] In some embodiments, the user's device 411 may include a database with at least one data packet type corresponding to a request for sharing of data packets 403 from the user's device 411, wherein the type of data packets 403 may be determined from the data packet type database. In some embodiments, at least one response may be linked to a type of data packet 403 from the user's device 411, wherein the linking may be based on the data type and data pattern of the at least one response.

[076] In some embodiments, a response corresponding to a request for sharing of data packets may be identified (e.g., by a processor 402), wherein the identified response is not compatible with the received privacy preference. In some embodiments, a response with at least one modified data packet corresponding to the request for sharing types of data packets may be provided per the modification algorithm. In some embodiments,

modification of the at least one modified data packet 403 may be selected from the group consisting of data nullification, change of encoding and/or file template, change of header and/or footer, blocking, data randomization, content modification, addition of a predetermined data packet, encryption or the like.

[077] In some embodiments, a communication pattern between the server 401 and the user's device 411 may be identified, wherein the communication pattern may include at least one request for retrieval of at least one data packet 403 from the user's device 411 and corresponding responses. In some embodiments, an alert may be issued (e.g., by a processor 402) upon detection of a change in the identified communication pattern. In some embodiments, data packets 403 from the user's device 411 may be a response created as full or partial extraction(s) selected from the group consisting of any one of user's device files (permanent or temporary), user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory user's device static memory or the like. .

[078] Reference is now made to Fig. 6B, which shows a flowchart for a method of dynamic management of private data during communication between a remote server 401 and a user's device 411, according to some embodiments of the invention. In some embodiments, user's device 411 may receive 611 a request for retrieval of at least one data packet 403 from the user's device 411, wherein the user's device 411 may provide a response corresponding to the received request.

[079] In some embodiments, user's device 411 may determine 612 at least one data pattern corresponding to the received request. In some embodiments, user's device 411 may receive 613 a privacy preference for the user's device 411, wherein the privacy preference may include a list of allowed (and/or forbidden) data patterns for sharing (and/or randomly modifying according to the predetermined modification algorithm for each of the forbidden data patterns) during communication. In some embodiments, responses corresponding to requests for sharing of data packets and corresponding data patterns that are not compatible with the received privacy preference may be modified 614. In some embodiments, communication between the remote server 401 and the user's device 411 may be maintained 615 with sharing of the modified responses.

[080] In some embodiments, user's device 411 may determine the type of the at least one data packet 403 of the received request. In some embodiments, requests for sharing of data

packets 403 and corresponding data patterns, corresponding to at least one data packet type, that are not compatible with the received privacy preference may be modified. In some embodiments, the privacy preference may include a list of allowed (and/or forbidden) data packet types for sharing (and/or modifying) during communication.

[081] In some embodiments, user's device 411 may include a database with at least one data pattern corresponding to a request for sharing of data packets from the user's device, and wherein the at least one data pattern compatible with the received request may be determined from the database. In some embodiments, user's device 411 may determine the type of the at least one data packet 403 of the received request, and link at least one data pattern to a type of data packet from the user's device 411, wherein the linking may be based on the pattern of the at least one response.

[082] In some embodiments, a data pattern corresponding to a request for sharing of types data packets 403 may be identified (e.g., by a processor 402), wherein the identified data pattern is not compatible with the received privacy preference. In some embodiments, a response with at least one modified data packet corresponding to the request for sharing types of data packets may be provided.

[083] In some embodiments, an alert may be issued (e.g., by a processor 402) upon detection of a request for sharing data packets, wherein the detected request does not correspond to a data type and/or a data pattern and/or a combination thereof that is not compatible with the received privacy preference. In some embodiments, a communication pattern between the server 401 and the user's device 411 may be identified, wherein the communication pattern may include at least one request for retrieval of at least one data packet 403 from the user's device 411 and corresponding responses. In some embodiments, an alert may be issued (e.g., by a processor 402) upon detection of a change in the identified communication pattern.

[084] In some embodiments, a data management system (e.g., data management system 400 as shown in Fig. 4) may be implemented as an exit gatekeeper to monitor outflow communication. For example, in network embedded devices (NED) with limited CPU power, low memory capacity and low power resources means (e.g., internet of things (IOT) device and/or machine to machine and/or machine to server communication and/or other thin client or the like). Outflow communication may be monitored for communication patterns and/or data packet type and/or data pattern and once going out of

predefined type and/or pattern range, may limit communication flow and/or block it. This ability to monitor and control outflow communication by the system may prevent for any user's device and/or NED, from being part of communication overloading attacks for example distributed denial of service (DDoS) attack or the like. Such attacks may be created by malicious attackers who are remotely using uncontrolled user's device and/or NED or the like, to generate very high communication flow (e.g., 1 terabyte per second) in short period of time (e.g. hundreds of thousands or more of IP address endpoints at the same time) that basically overload the attacked server(s) until it adversely impacts its ability to function and in some cases creates fatal malfunction in mission critical systems.

[085] Reference is now made to Fig. 7, which schematically illustrates a data management system 700 for dynamic management of private data that is at least partially embedded on a hardware component 711 (indicated with a solid line), according to some embodiments of the invention. The data management system 700 may include the communication module and/or processor adjusted and preconfigured to privacy preference methods and processes and/or data storage such as privacy preference database. The data management system 700 may be at least partially embedded on a hardware component 711, for instance embedded on one chip and/or integrated circuit and/or processor. According to some embodiments the system may communicate with server 401 and/or user's device 411 via the communication module 412. In some embodiments, the hardware component 711 (indicated with a solid line) may include at least one privacy preference database that been preconfigured and may be updated only locally so that no remote change can be made, for example by using electrically erasable programmable read-only memories (EEPROMs). In some embodiments, the hardware component 711 (indicated with a solid line) may be embedded and/or added to user's device 411 (indicated with a dashed line).

[086] For example, such data management system 700 may be added into an IOT device (e.g., adding a chip and/or a circuit to the CPU) such that DDoS may be prevented, for example, communication between the IOT device may be monitored and controlled for unusual communication patterns, such that data patterns containing higher frequency (e.g. higher than ten data packets per second) and/or data flow (e.g., higher than 1megabyte per second) may be blocked by the system, according to privacy preferences determined for that purpose. For example, as shown in Fig. 3C as well. It should be noted that such

preferences may only check data patterns where the data type of the data packets in the communication are not checked.

[087] Unless explicitly stated, the method embodiments described herein are not constrained to a particular order in time or chronological sequence. Additionally, some of the described method elements can be skipped, or they can be repeated, during a sequence of operations of a method.

[088] Various embodiments have been presented. Each of these embodiments may of course include features from other embodiments presented, and embodiments not specifically described may include various features described herein.

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92*bis*.1 and Administrative Instructions, Section 422)

To:

FRYDMAN, Idan
Pearl Cohen Zedek Latzer Baratz
P.O. Box 7198
6107121 Tel Aviv
ISRAËL

Date of mailing *(day/month/year)*
24 April 2018 (24.04.2018)

Applicant's or agent's file reference
P-566702-PC

IMPORTANT NOTIFICATION

International application No.
PCT/IL2018/050359

International filing date *(day/month/year)*
28 March 2018 (28.03.2018)

1. The following indications appeared on record concerning:

☐ the applicant ☒ the inventor ☐ the agent ☐ the common representative

Name and Address

VAAKNIN, David
61 Nof-Harim Street
44862 Zur Yigal
Israel

State of Nationality | State of Residence

Telephone No.

Facsimile No.

E-mail address

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☐ the name ☐ the address ☐ the nationality ☐ the residence

Name and Address

State of Nationality | State of Residence

Telephone No.

Facsimile No.

E-mail address
☐ Notifications by e-mail authorized

3. Further observations, if necessary:
Inventor in box 1. is no longer recorded.

4. A copy of this notification has been sent to:

☒ the receiving Office
☐ the International Searching Authority
☐ the Authority(ies) specified for supplementary search
☐ the International Preliminary Examining Authority
☐ the designated Offices concerned
☐ the elected Offices concerned
☒ other: VAAKNIN, David

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 71 30

Authorized officer
Fahy Laurence
e-mail pct.team9@wipo.int
Telephone No. +41 22 338 74 09

P-566702-PC

PCT REQUEST

Print Out (Original in Electronic Form)

0	**For receiving Office use only**	
0-1	International Application No.	**PCT/IL2018/050359**
0-2	International Filing Date	**28 March 2018 (28.03.2018)**
0-3	Name of receiving Office and "PCT International Application"	**RO/IL**

0-4	**Form PCT/RO/101 PCT Request**	
0-4-1	Prepared Using	PCT-SAFE Version 3.51.080.256 MT/FOP 20180101/0.20.5.24
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	Israel Patent Office (RO/IL)
0-7	**Applicant's or agent's file reference**	P-566702-PC
I	**Title of Invention**	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA
II	**Applicant**	
II-1	This person is	Applicant only
II-2	Applicant for	All designated States
II-4	Name (LAST, First)	KOREN, Yoseph
II-5	Address	91/33 Hagalil street 5591491 Ganey-Tikva Israel
II-6	State of nationality	IL
II-7	State of residence	IL
III-1	**Applicant and/or inventor**	
III-1-1	This person is	Inventor only
III-1-3	Inventor for	All designated States
III-1-4	Name (LAST, First)	VAAKNIN, David
III-1-5	Address	61 Nof-Harim Street 44862 Zur Yigal Israel
III-2	**Applicant and/or inventor**	
III-2-1	This person is	Inventor only
III-2-3	Inventor for	All designated States
III-2-4	Name (LAST, First)	WASSERMAN, Yehonatan
III-2-5	Address	39 Kaplan St. 5529339 Kiryat-Ono Israel

P-566702-PC

PCT REQUEST

Print Out (Original in Electronic Form)

IV-1	**Agent or common representative; or address for correspondence**	
	The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	Agent
IV-1-1	Name	PEARL COHEN ZEDEK LATZER BARATZ
IV-1-2	Address	P.O. Box 7198 6107121 Tel Aviv Israel
IV-1-3	Telephone No.	+972-3-3039000
IV-1-4	Facsimile No.	+972-3-3039001
IV-1-5	e-mail	PCT@pearlcohen.com
IV-1-5(a)	E-mail authorization The receiving Office, the International Searching Authority, the International Bureau and the International Preliminary Examining Authority are authorized to use this e-mail address, if the Office or Authority so wishes, to send notifications issued in respect of this international application:	exclusively in electronic form (no paper notifications will be sent)
IV-1-6	Agent's registration No.	557802576
IV-2	**Additional agent(s)**	additional agent(s) with same address as first named agent
IV-2-1	Name(s)	FRYDMAN, Idan
V	**DESIGNATIONS**	
V-1	**The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.**	
VI-1	**Priority claim of earlier national application**	
VI-1-1	Filing date	09 April 2017 (09.04.2017)
VI-1-2	Number	251683
VI-1-3	Country or Member of WTO	IL
VI-2	**Priority document request**	
	The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s):	VI-1

P-566702-PC

PCT REQUEST

Print Out (Original in Electronic Form)

VI-3	**Incorporation by reference :** where an element of the international application referred to in Article 11(1)(iii)(d) or (e) or a part of the description, claims or drawings referred to in Rule 20.5(a) is not otherwise contained in this international application but is completely contained in an earlier application whose priority is claimed on the date on which one or more elements referred to in Article 11(1)(iii) were first received by the receiving Office, that element or part is, subject to confirmation under Rule 20.6, incorporated by reference in this international application for the purposes of Rule 20.6.		
VII-1	**International Searching Authority Chosen**	Israel Patent Office (ISA/IL)	
VIII	**Declarations**	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	–	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	–	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	–	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	–	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	–	
IX	**Check list**	Number of sheets	Electronic file(s) attached
IX-1	Request (including declaration sheets)	4	✓
IX-2	Description	24	✓
IX-3	Claims	7	✓
IX-4	Abstract	1	✓
IX-5	Drawings	10	✓
IX-7	TOTAL	46	

P-566702-PC

PCT REQUEST

Print Out (Original in Electronic Form)

	Accompanying Items	Paper document(s) attached	Electronic file(s) attached
IX-8	Fee calculation sheet	–	✓
IX-19	Other	Documents in pre-conversion format Statement (Section 706): This is a complete and accurate copy of the international application prior to its conversion into the electronic document format in which it is filed.	✓
IX-19	Other	Sub Agent List	✓
IX-20	**Figure of the drawings which should accompany the abstract**	5	
IX-21	**Language of filing of the international application**	English	
X-1	**Signature of applicant, agent or common representative**	(PKCS7 Digital Signature)	
X-1-1	Name	PEARL COHEN ZEDEK LATZER BARATZ	
X-1-2	Name of signatory	FRYDMAN, Idan	
X-1-3	Capacity (if such capacity is not obvious from reading the request)	Agent	

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	**28 March 2018 (28.03.2018)**
10-2	**Drawings:**	
10-2-1	Received	
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/IL
10-6	**Transmittal of search copy delayed until search fee is paid**	V

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	

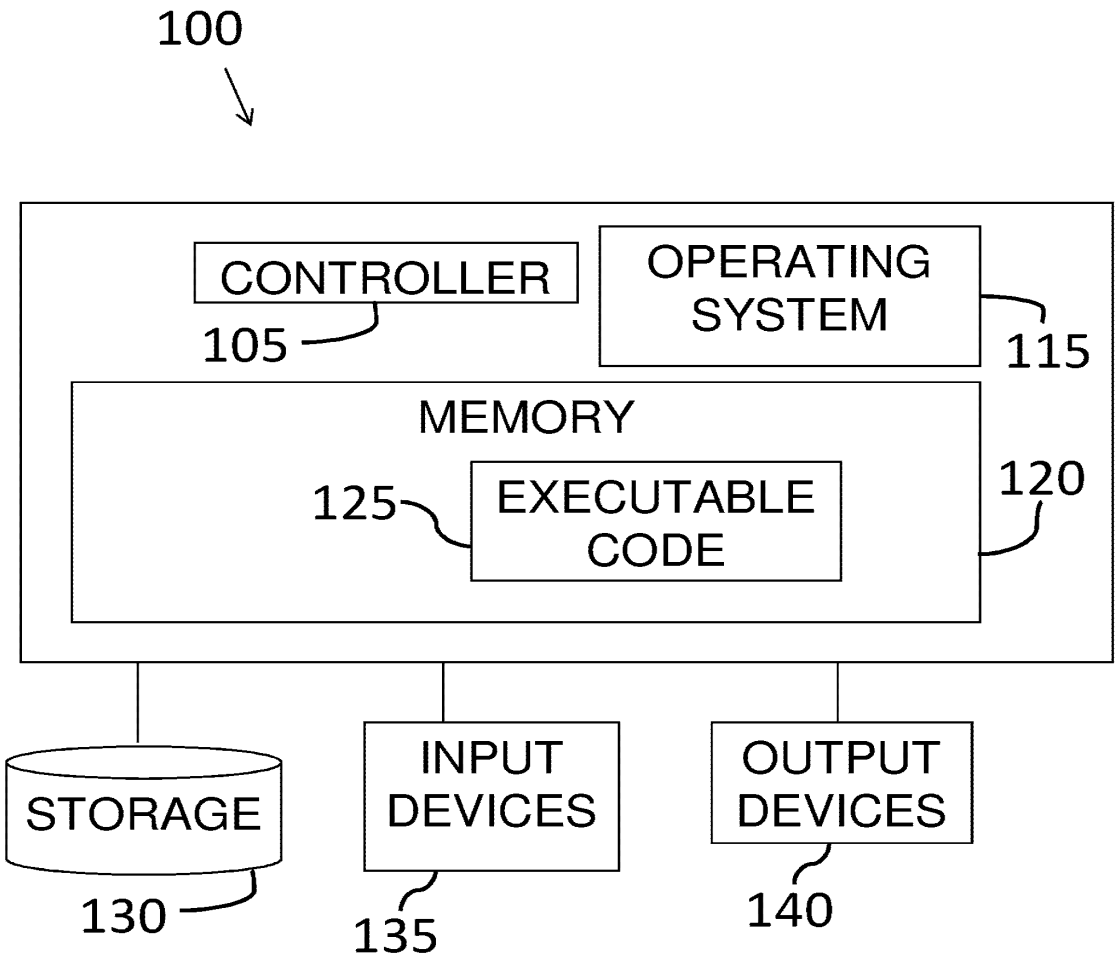

100
CONTROLLER
105
OPERATING SYSTEM
115
MEMORY
125
EXECUTABLE CODE
120
STORAGE
130
INPUT DEVICES
135
OUTPUT DEVICES
140

Fig. 1

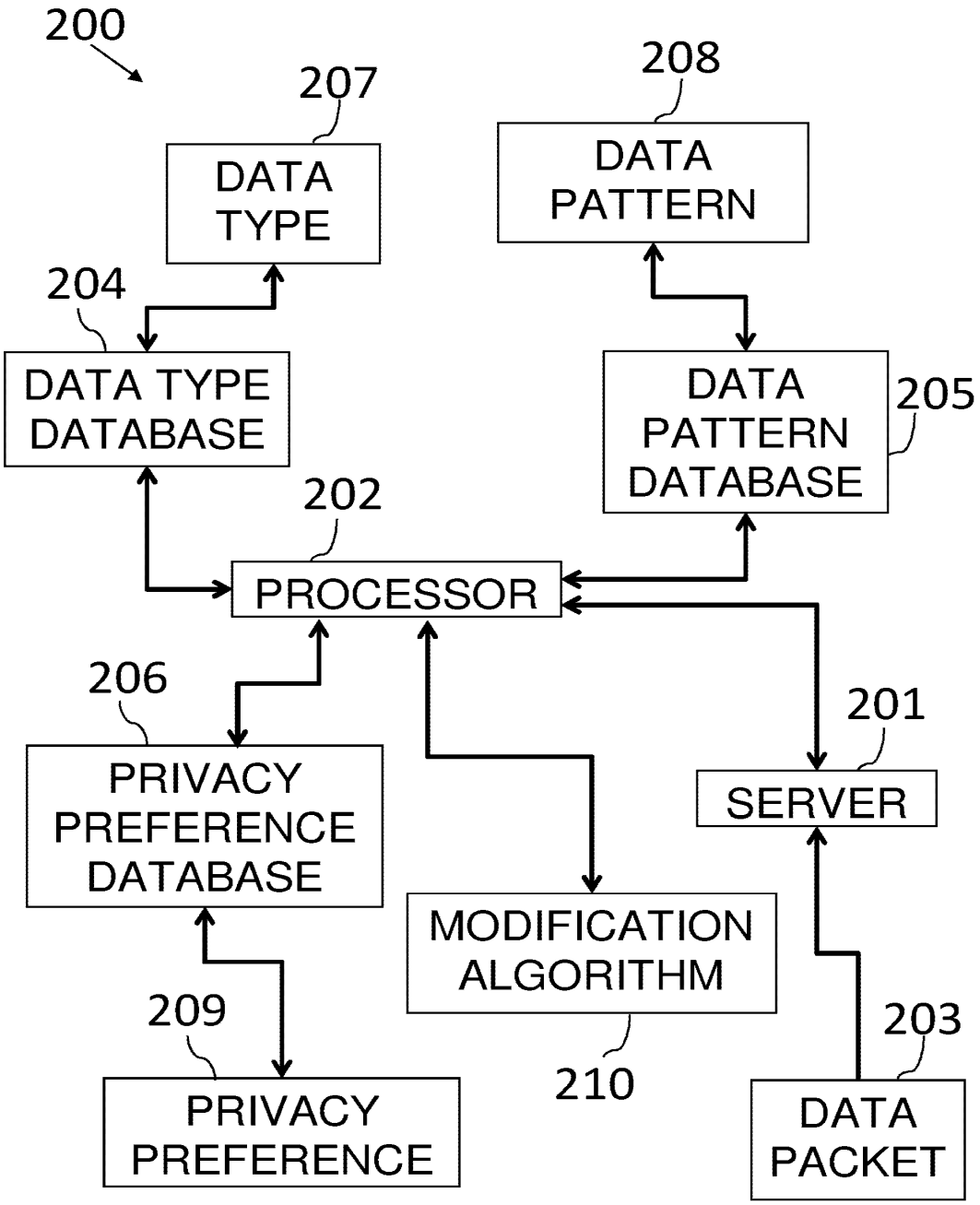

200
207
DATA TYPE
208
DATA PATTERN
204
DATA TYPE DATABASE
DATA PATTERN DATABASE
205
202
PROCESSOR
206
201
PRIVACY PREFERENCE DATABASE
SERVER
MODIFICATION ALGORITHM
209
203
210
PRIVACY PREFERENCE
DATA PACKET

Fig. 2

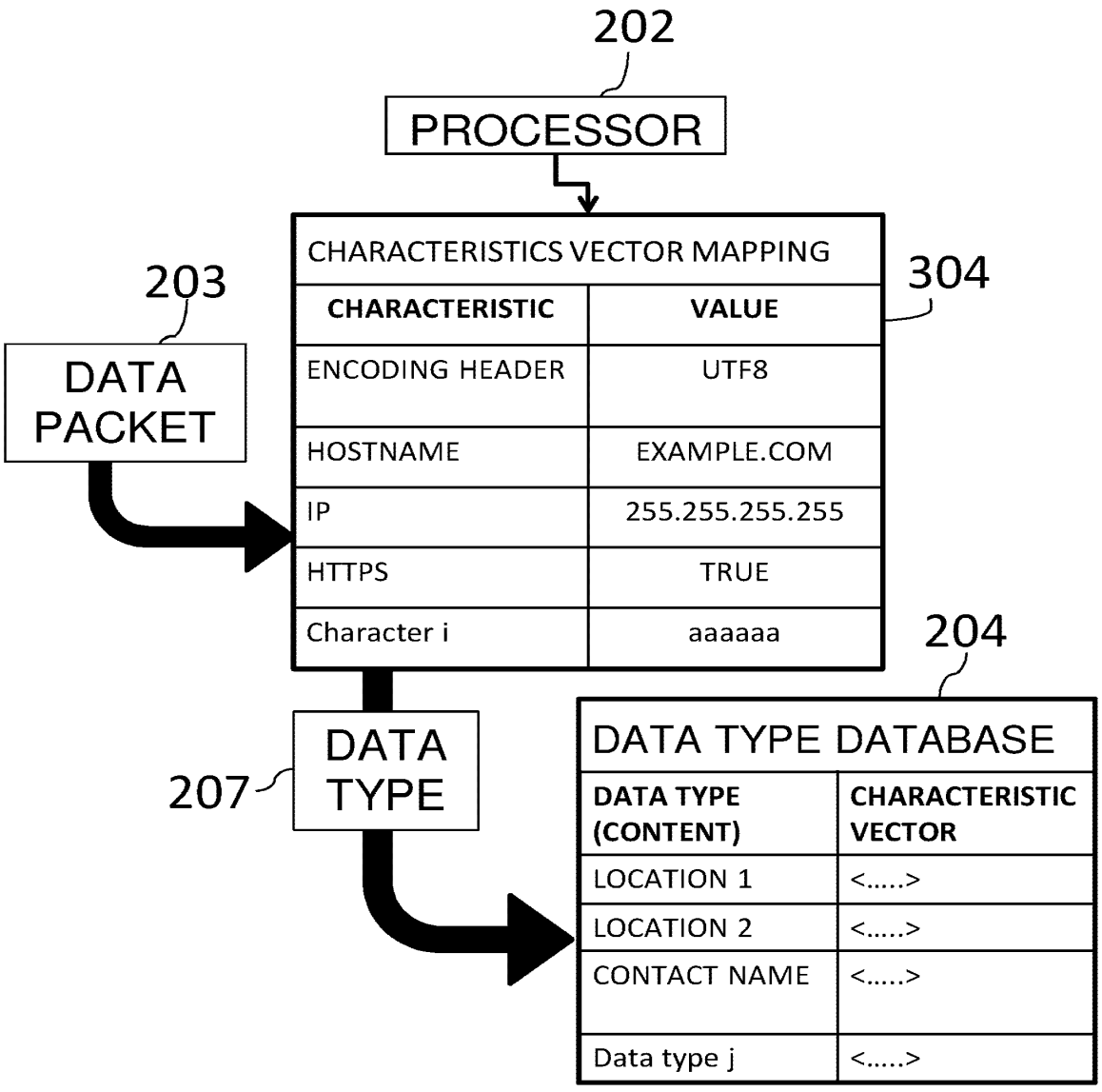

202
PROCESSOR
CHARACTERISTICS VECTOR MAPPING
304
203
DATA PACKET
CHARACTERISTIC
VALUE
ENCODING HEADER
UTF8
HOSTNAME
EXAMPLE.COM
IP
255.255.255.255
HTTPS
TRUE
Character i
aaaaaa
204
DATA TYPE DATABASE
207
DATA TYPE
DATA TYPE (CONTENT)
CHARACTERISTIC VECTOR
LOCATION 1
<.....>
LOCATION 2
<.....>
CONTACT NAME
<.....>
Data type j
<.....>

Fig.3A

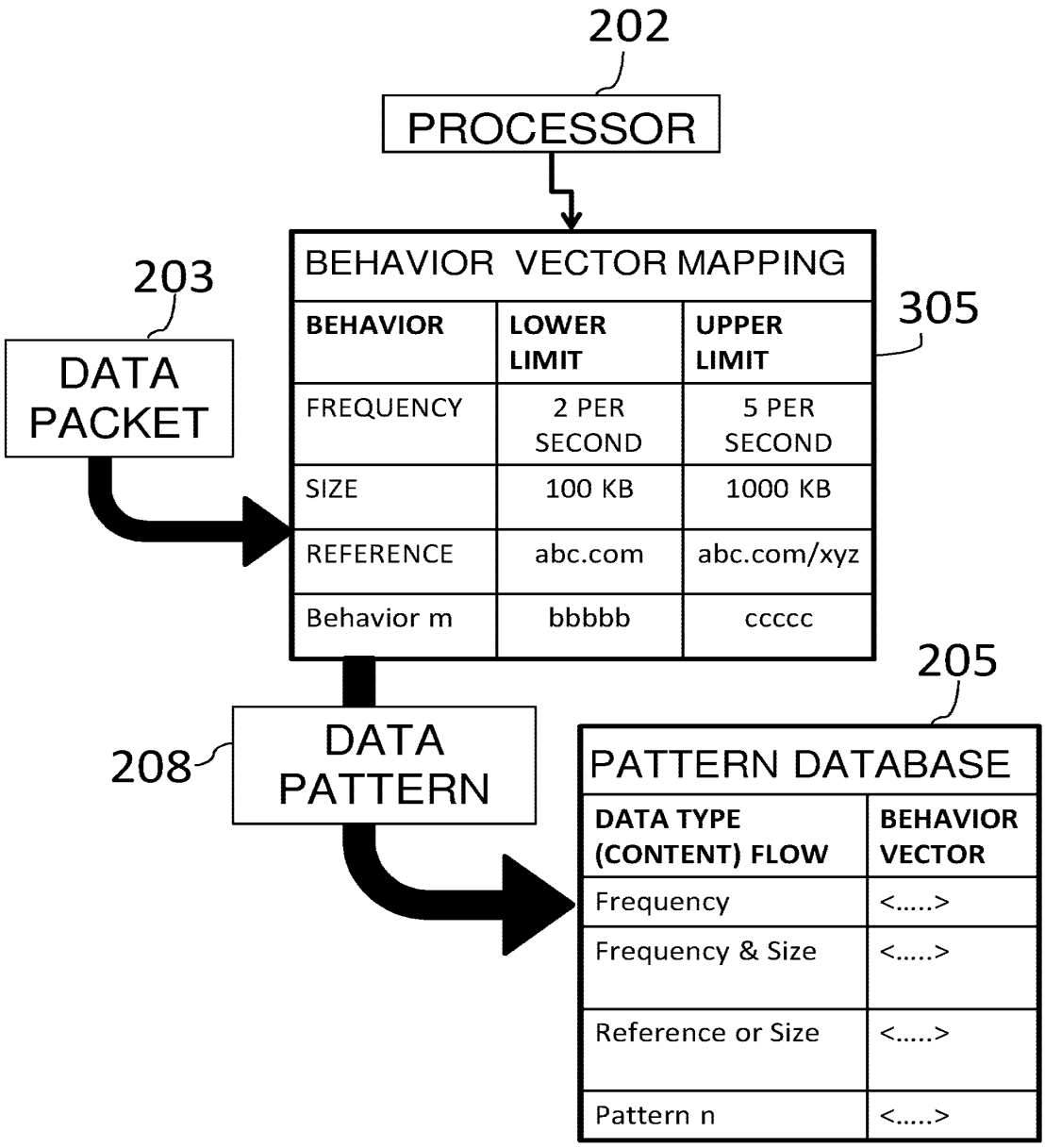
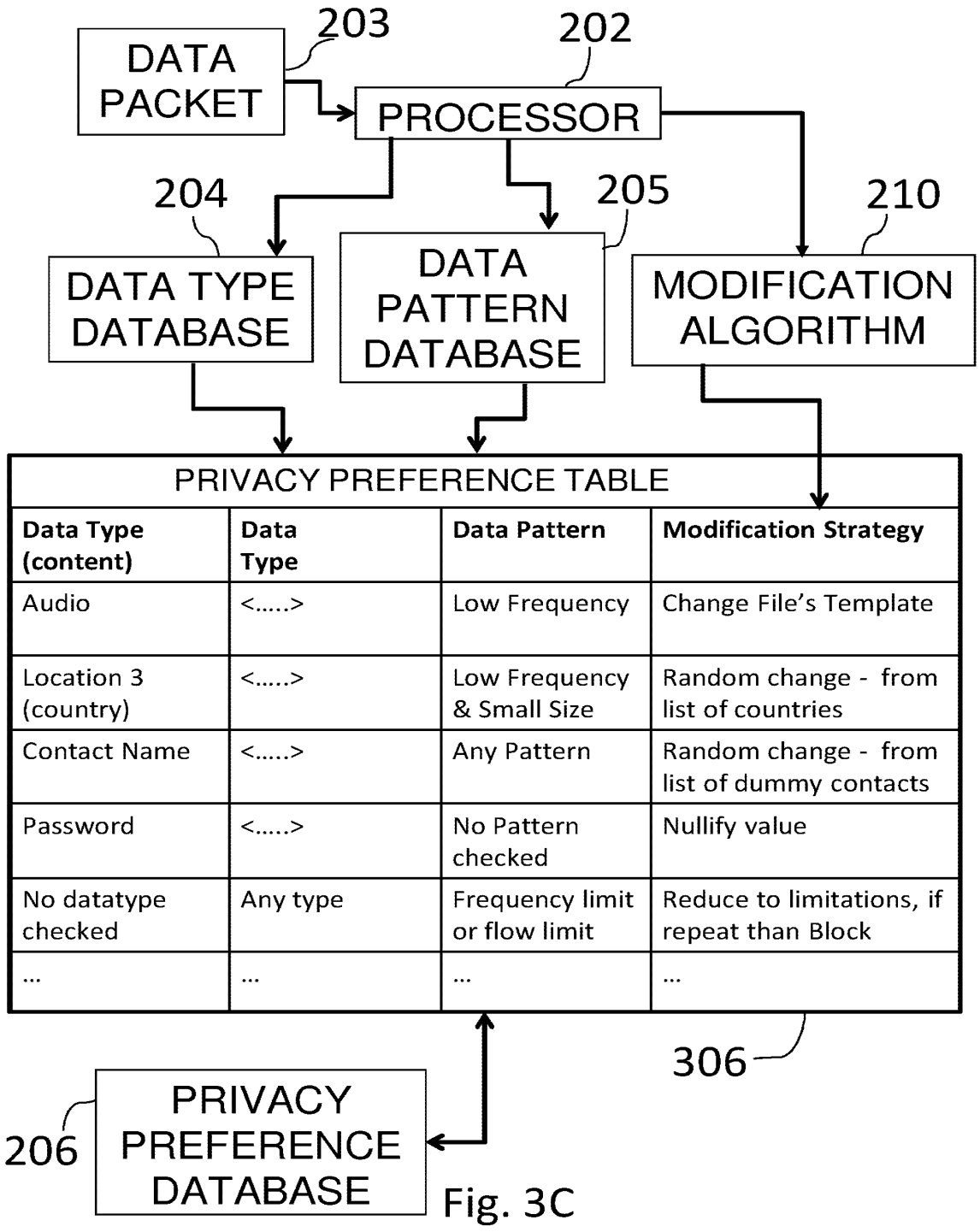

202
PROCESSOR
203
DATA PACKET
BEHAVIOR VECTOR MAPPING
305
BEHAVIOR
LOWER LIMIT
UPPER LIMIT
FREQUENCY
2 PER SECOND
5 PER SECOND
SIZE
100 KB
1000 KB
REFERENCE
abc.com
abc.com/xyz
Behavior m
bbbbb
ccccc
205
208
DATA PATTERN
PATTERN DATABASE
DATA TYPE (CONTENT) FLOW
BEHAVIOR VECTOR
Frequency
<.....>
Frequency & Size
<.....>
Reference or Size
<.....>
Pattern n
<.....>

Fig. 3B



Data Type (content)	Data Type	Data Pattern	Modification Strategy
Audio	<.....>	Low Frequency	Change File's Template
Location 3 (country)	<.....>	Low Frequency & Small Size	Random change - from list of countries
Contact Name	<.....>	Any Pattern	Random change - from list of dummy contacts
Password	<.....>	No Pattern checked	Nullify value
No datatype checked	Any type	Frequency limit or flow limit	Reduce to limitations, if repeat than Block
...	...	...	...

Fig. 3C

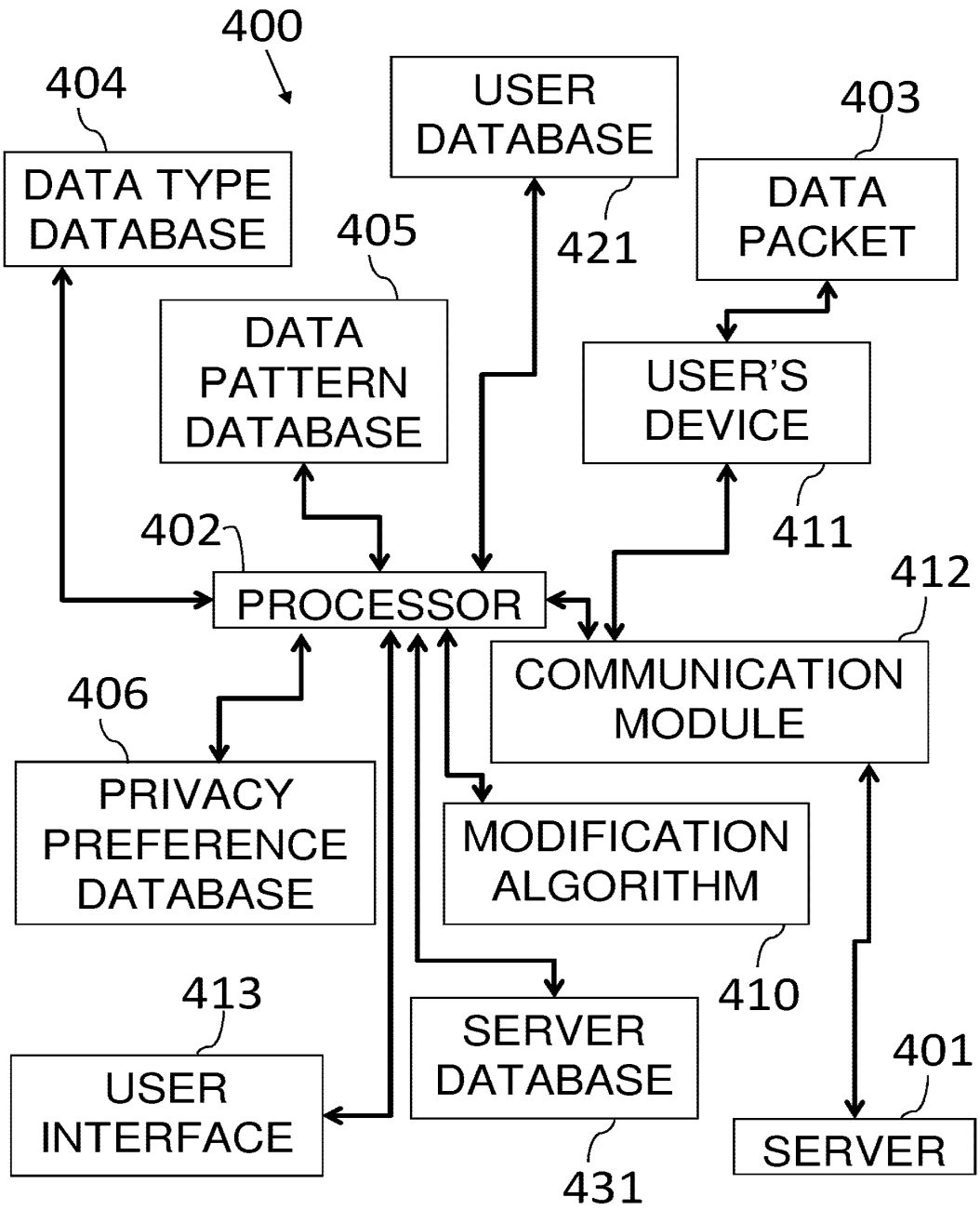

400
404
DATA TYPE DATABASE
USER DATABASE
421
403
DATA PACKET
405
DATA PATTERN DATABASE
USER'S DEVICE
411
402
PROCESSOR
412
COMMUNICATION MODULE
406
PRIVACY PREFERENCE DATABASE
MODIFICATION ALGORITHM
410
413
USER INTERFACE
SERVER DATABASE
431
401
SERVER

Fig. 4

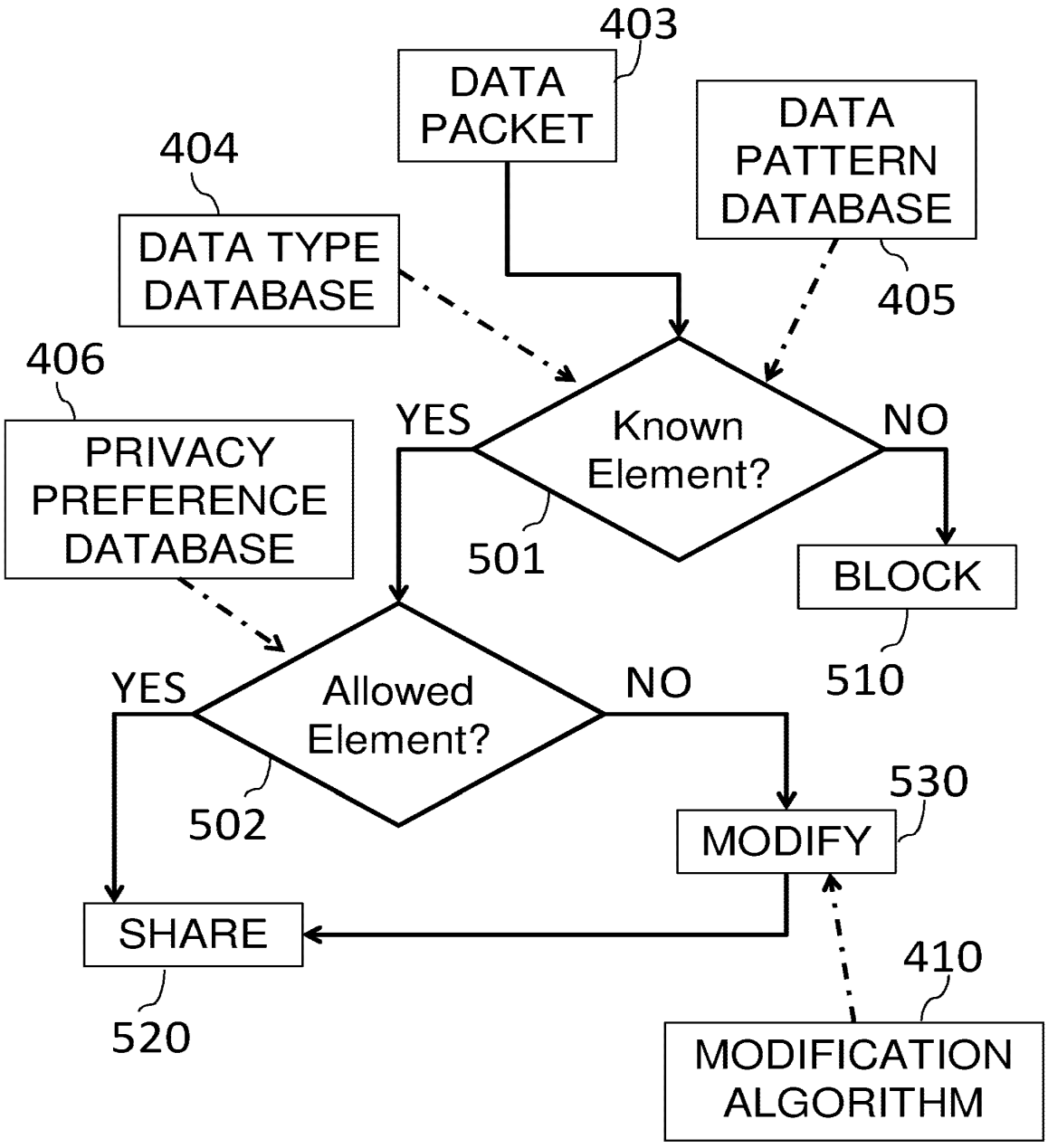

403
DATA PACKET
DATA PATTERN DATABASE
404
DATA TYPE DATABASE
405
406
PRIVACY PREFERENCE DATABASE
YES
Known Element?
NO
501
BLOCK
510
YES
Allowed Element?
NO
502
530
MODIFY
SHARE
520
410
MODIFICATION ALGORITHM

Fig. 5

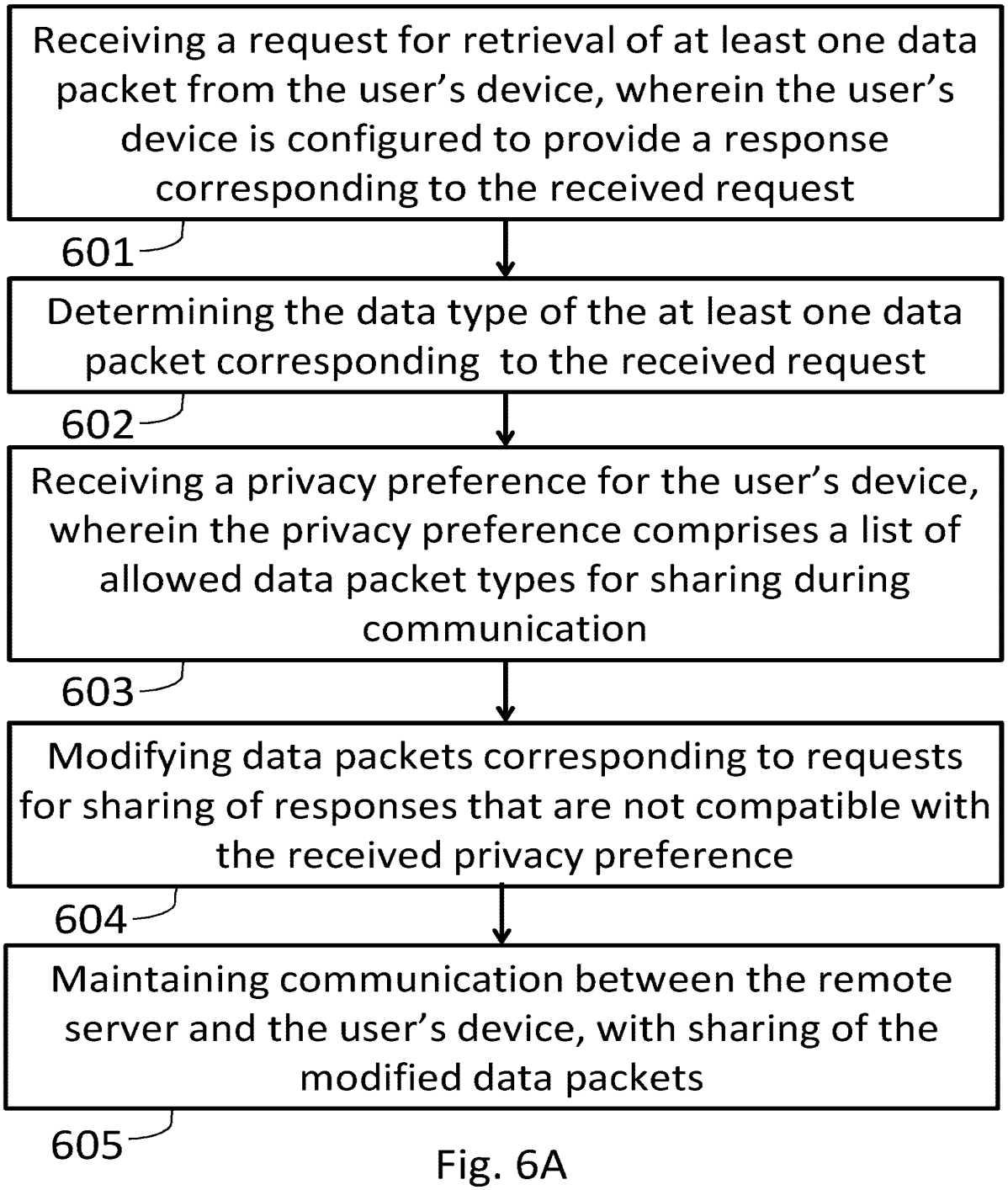

Receiving a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request
601
Determining the data type of the at least one data packet corresponding to the received request
602
Receiving a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet types for sharing during communication
603
Modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference
604
Maintaining communication between the remote server and the user's device, with sharing of the modified data packets
605

Fig. 6A

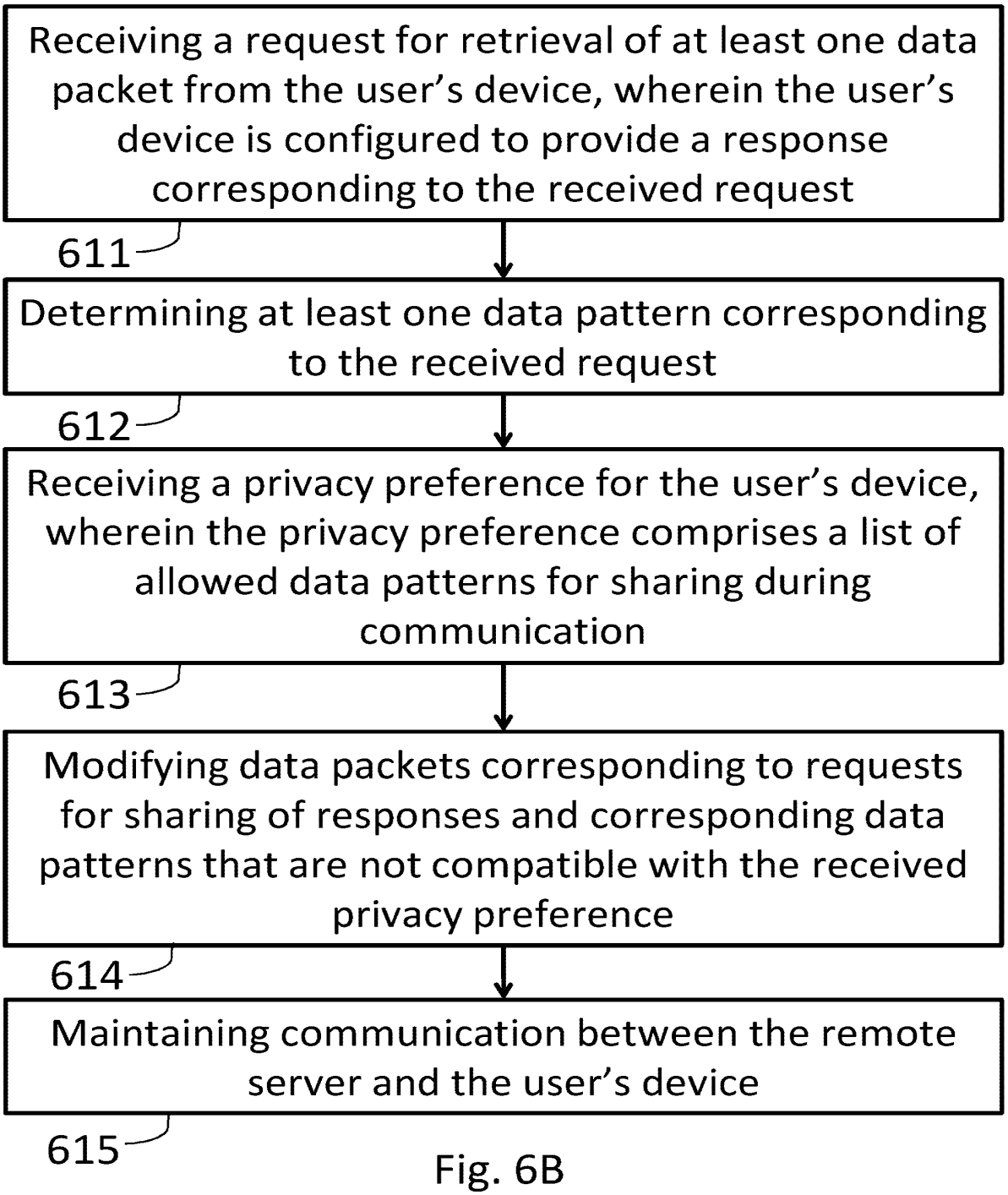

Receiving a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request
611
Determining at least one data pattern corresponding to the received request
612
Receiving a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data patterns for sharing during communication
613
Modifying data packets corresponding to requests for sharing of responses and corresponding data patterns that are not compatible with the received privacy preference
614
Maintaining communication between the remote server and the user's device
615

Fig. 6B

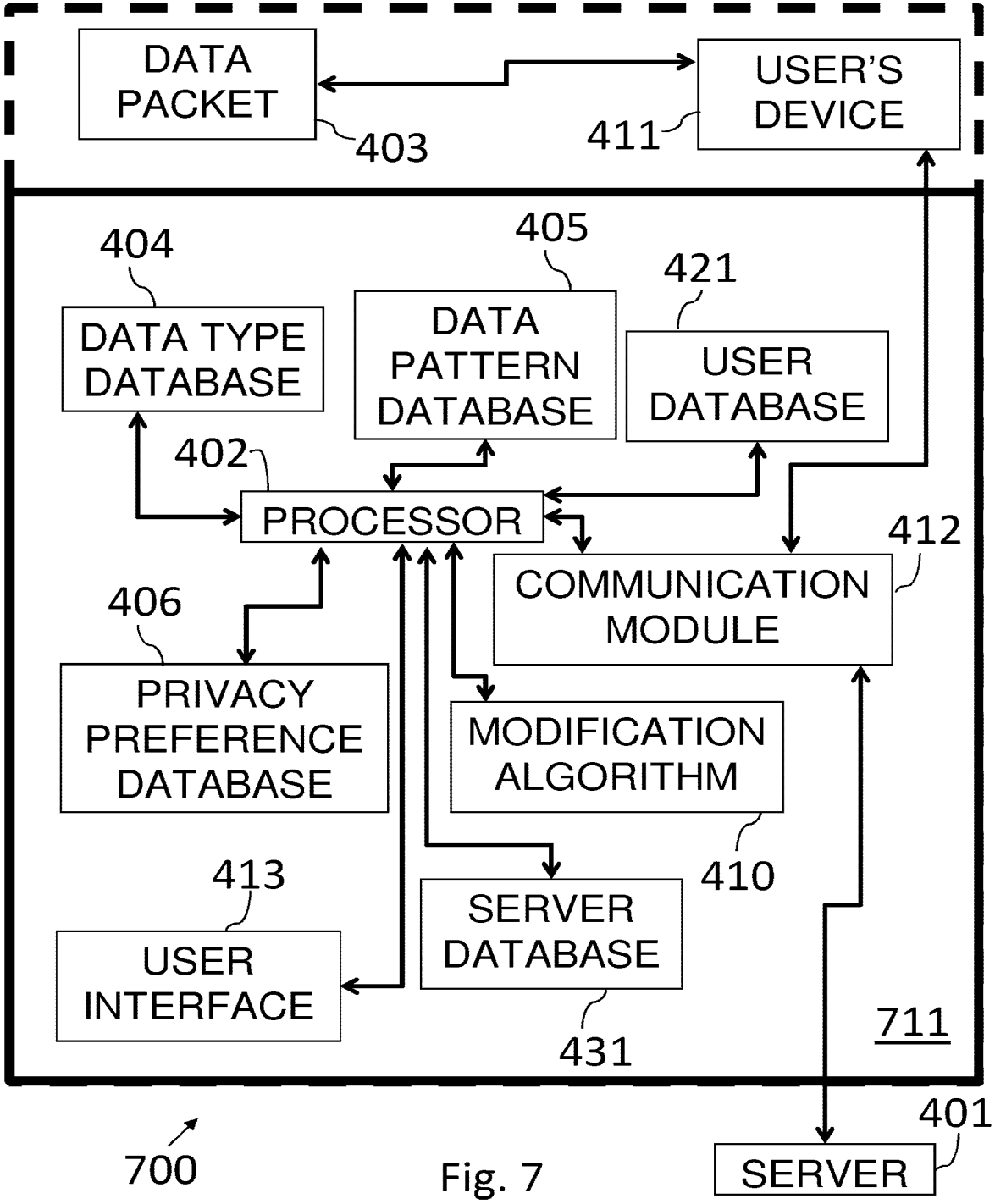

DATA PACKET
403
USER'S DEVICE
411
404
DATA TYPE DATABASE
405
DATA PATTERN DATABASE
421
USER DATABASE
402
PROCESSOR
412
COMMUNICATION MODULE
406
PRIVACY PREFERENCE DATABASE
MODIFICATION ALGORITHM
410
413
USER INTERFACE
SERVER DATABASE
431
711
401
SERVER
700

Fig. 7

רשות הפטנטים

מדינת ישראל
משרד המשפטים

זאת לאשר כי רצופים בזה העתקים נכונים של המסמכים שהופקדו לכתחילה עם הבקשה לפטנט אשר פרטיה רשומים בעמוד הראשון של הנספח.

This is to certify that annexed hereto is a true copy of the documents as originally deposited with the patent application of which particulars are specified on the first page of the annex.

This 10 APR 2018 היום

Ofir Alon אופיר אלון
רשם הפטנטים
המדגמים וסימני המסחר
Commissioner of Patents
Designs and Trademarks

State of Israel
Patent Office

אישור הגשת בקשה
Filing Receipt

מדינת ישראל
רשות הפטנטים

Confidential for applicant only — **שמור למבקש בלבד**

Application No:	251683	**מספר בקשה:**
Date of application:	09/04/2017	**תאריך הבקשה:**
Date of submission:	09/04/2017	**תאריך הגשה:**

SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

מערכת ושיטה לניהול דינאמי של נתונים פרטיים

Patentee(s):	**בעלי הפטנט:**
KOREN, Yoseph Customer No: 923084 91 HAGALIL STREET GANEY-TIKVA, 5591491 ISRAEL	יוסף קורן קוד לקוח:923084 הגליל 91 גני תקווה 5591491 ישראל
Inventor(s):	**ממציא(ים):**
KOREN, Yoseph Customer No: 923085	קוד לקוח:923085
WASSERMAN, Yehonatan Customer No: 923086	קוד לקוח:923086

Address for service: — **המען למסירת הודעות:**

PEARL COHEN ZEDEK LATZER BARATZ
5 SHENKAR ST.,
P.O.B. 12704,
HERZLIYA 4673339
Israel
ipomail@pczlaw.com

פרל כהן צדק לצר ברץ
מרכז גב-ים 1, רח' שנקר 5
ת.ד. 12704
הרצליה 4673339
ישראל
ipomail@pczlaw.com

Reference:	P-566702-IL	סימוכין:
Invention owner by:	inventorship בהיותי הממציא	המצאה מכח:

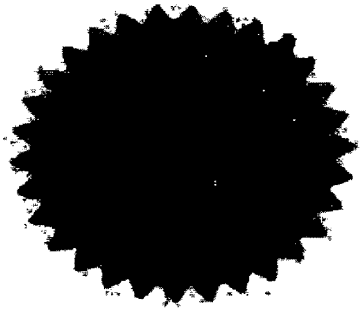
אישור זה כשהוא חתום בחותמת רשות הפטנטים מהווה אישור הגשת בקשה בלבד זאינו מהווה תעודה המעידה על רישום הפטנט. במידה ונמצא שיבוש בקליטת הנתונים כפי שהם מופיעים באישור זה הינכם מתבקשים להעיר את הערותיכם תוך עשרה ימים מהיום.

State of Israel
Patent Office

אישור הגשת בקשה

Filing Receipt

מדינת ישראל
רשות הפטנטים



Register of Patents

As of

20/04/2017

רשם הפטנטים

מצב ליום

Ex.1002 / Page 289 of 418
Cisco Systems, Inc.

P-566702-IL

SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

FIELD OF THE INVENTION

[001] The present invention relates to data management. More particularly, the present invention relates to systems and methods for dynamic management of private data.

BACKGROUND OF THE INVENTION

[002] During communication with external remote servers different types of data are automatically (and uncontrollably) shared, sometimes without the knowledge of the user (e.g., the owner of the data). There are currently only limited ways for the user to manage which data should be shared, with which parties, and at what time periods and/or under what circumstances such that privacy agreements cannot be fully enforced. For example, securing private elements of a user's device engaging in a transaction with a service provider, has been a challenge for many years with the rapid development of computer technology.

[003] In recent years, an increasing number of communication sessions are being biased (in terms of shared data and application usage) toward one party which is advantageous due to technological superiority, formal regulation power, and/or any other item. Such biasing may occur due to rapid development of communication related software, as well as due to development of computer technology.

[004] Social network service providers usually collect user (private) data, for example collect user's online habits. Data collection is usually carried out by a service provider requesting to share user's (private) information while the user's device automatically shares the requested information accordingly. Actions are executed by dedicated software (e.g., social plug in), which upload data requests when visiting web sites and/or applications. Such requests may be direct script by the service provider (e.g. cookie etc.), or indirect script hidden within links to other (partner) application provider (e.g. social plug-in, SDK, API etc.). While some devices allow blocking collection of certain private parameters, for example the location, only data emerging from sensors, such as global positioning system (GPS) sensors, can be managed by user while other sources of location (e.g. mobile network, IP provider, country, time zone) cannot be controlled so that in that case location information can still be collected. Thus, location information can be collected

while bypassing the instructions of the user (e.g., collecting location from cellular carrier data). Other examples from the same nature may include retrieving form data, retrieving data from flash memory and several other items which do not have the full (or partial) ability to disable and/or block data collection. Some service providers can also collect user data in order to transfer and/or sell to third parties (e.g., to present dedicated ads in the future). Another example may be avoiding biased exchange of information both from the user and the service provider perspectives.

SUMMARY OF THE INVENTION

[005] There is thus provided, in accordance with some embodiments of the invention, a method of dynamic management of private data during communication between a remote server and a user's device, the method including receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request, determining, by the user's device, the data type of the at least one data packet corresponding to the received request, receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference includes a list of allowed data packet types for sharing during communication, modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference, and maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

[006] In some embodiments, the type of the at least one data packet may be determined from metadata of communication with the remote server. In some embodiments, the method further includes determining, by the user's device, pattern of at least one response corresponding to the received request, and modifying data packets corresponding to requests for sharing of responses, corresponding to at least one data pattern, that are not compatible with the received privacy preference, wherein the privacy preference includes a list of allowed data patterns for sharing during communication. In some embodiments, the user's device includes a database with at least one data packet type corresponding to a request for sharing of data packets from the user's device, and wherein the type of data packets is determined from the database.

[007] In some embodiments, the method further includes linking at least one response to a type of data packet from the user's device, wherein the linking is based on the type and pattern of the at least one response. In some embodiments, the method further includes identifying a response corresponding to a request for sharing of data packets, wherein the identified response is not compatible with the received privacy preference, and providing a response with at least one modified data packet corresponding to the request for sharing types of data packets. In some embodiments, the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

[008] In some embodiments, the method further includes identifying a communication pattern between the server and the user's device, wherein the communication pattern includes at least one request for retrieval of at least one data packet from the user's device and corresponding responses, and issuing an alert upon detection of a change in the identified communication pattern.

[009] In some embodiments, data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

[010] There is thus provided, in accordance with some embodiments of the invention, a method of dynamic management of private data during communication between a remote server and a user's device, the method including receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request, determining, by the user's device, at least one data pattern corresponding to the received request, receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference includes a list of allowed data patterns for sharing during communication, modifying data packets corresponding to requests for sharing of responses and corresponding data patterns that are not compatible with the received privacy preference, and maintaining communication between the remote server and the user's device, with sharing of the modified responses.

[011] In some embodiments, the pattern of the at least one response is determined from metadata of communication with the remote server. In some embodiments, the method further includes determining, by the user's device, the type of the at least one data packet of the received request, and modifying data packets corresponding to requests for sharing of responses and corresponding data patterns, corresponding to at least one data packet type, that are not compatible with the received privacy preference, wherein the privacy preference includes a list of allowed data packet types for sharing during communication.

[012] In some embodiments, the user's device includes a database with at least one data pattern corresponding to a request for sharing of data packets from the user's device, and wherein the at least one data pattern compatible with the received request is determined from the database. In some embodiments, the method further includes determining, by the user's device, the type of the at least one data packet of the received request, and linking at least one data pattern to a type of data packet from the user's device, wherein the linking is based on the pattern of the at least one response.

[013] In some embodiments, the method further includes identifying a data pattern corresponding to a request for sharing of data packet types, wherein the identified data pattern is not compatible with the received privacy preference, and providing a response with at least one modified data packet corresponding to the request for sharing types of data packets. In some embodiments, the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

[014] In some embodiments, the method further includes issuing an alert upon detection of a request for sharing data packets, wherein the detected request does not correspond to at least one of data type and data pattern that is compatible with the received privacy preference. In some embodiments, the method further includes identifying a communication pattern between the server and the user's device, wherein the communication pattern includes at least one request for retrieval of at least one data packet from the user's device and corresponding responses, and issuing an alert upon detection of a change in the identified communication pattern.

[015] In some embodiments, data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect

attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

[016] There is thus provided, in accordance with some embodiments of the invention, a system for dynamic management of private data during communication between a remote server and at least one user's device, the system including a data type database, including at least one data type corresponding to sharing of at least one data packet from the user's device, a privacy preference database, including a list of allowed types of data packets for sharing during communication with the at least one user's device, a communication module, to allow communication between the remote server and the at least one user's device, and a processor, coupled to the response database and to the privacy preference database, wherein the processor is configured to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of data packets for sharing.

[017] In some embodiments, the system further includes a user interface to issue an alert upon detection of a request for retrieval of data packets that is not compatible with the privacy preference. In some embodiments, the system further includes a data pattern database, coupled to the processor, wherein the processor is configured to modify data packets corresponding to requests for retrieval of data packets and data types that are not compatible with data patterns from a data pattern database.

[018] In some embodiments, data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory. In some embodiments, at least the communication module and the processor are embedded on a single hardware component.

BRIEF DESCRIPTION OF THE DRAWINGS

[019] The subject matter regarded as the invention is particularly pointed out and distinctly claimed in the concluding portion of the specification. The invention, however, both as to organization and method of operation, together with objects, features, and advantages thereof, may best be understood by reference to the following detailed description when read with the accompanying drawings in which:

[020] Fig. 1 shows a schematic block diagram of an exemplary computing device, according to some embodiments of the invention;

[021] Fig. 2 schematically illustrates a data mapping system, according to some embodiments of the invention;

[022] Fig. 3A schematically illustrates examplary mapping of data type database, according to some embodiments of the invention;

[023] Fig. 3B schematically illustrates examplary mapping of data pattern database, according to some embodiments of the invention;

[024] Fig. 3C schematically illustrates examplary mapping of privacy preference table, according to some embodiments of the invention;

[025] Fig. 4 schematically illustrates a data management system, according to some embodiments of the invention;

[026] Fig. 5 shows a flowchart for a method of management of data packets with a sharing algorithm during communication between a remote server and a user's device, according to some embodiments of the invention;

[027] Figs. 6A-6B show flowcharts for a method of dynamic management of private data during communication between a remote server and a user's device, according to some embodiments of the invention; and

[028] Fig. 7 schematically illustrates a data management system 700 for dynamic management of private data that is embedded on a hardware component, according to some embodiments of the invention.

[029] It will be appreciated that for simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference numerals may be repeated among the figures to indicate corresponding or analogous elements.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[030] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will be understood by those skilled in the art that the present invention may be practiced without these specific

details. In other instances, well-known methods, procedures, and components have not been described in detail so as not to obscure the present invention.

[031] Although embodiments of the invention are not limited in this regard, discussions utilizing terms such as, for example, "processing," "computing," "calculating," "determining," "establishing", "analyzing", "checking", or the like, may refer to operation(s) and/or process(es) of a computer, a computing platform, a computing system, or other electronic computing device, that manipulates and/or transforms data represented as physical (e.g., electronic) quantities within the computer's registers and/or memories into other data similarly represented as physical quantities within the computer's registers and/or memories or other information non-transitory storage medium that may store instructions to perform operations and/or processes. Although embodiments of the invention are not limited in this regard, the terms "plurality" and "a plurality" as used herein may include, for example, "multiple" or "two or more". The terms "plurality" or "a plurality" may be used throughout the specification to describe two or more components, devices, elements, units, parameters, or the like. Unless explicitly stated, the method embodiments described herein are not constrained to a particular order or sequence. Additionally, some of the described method embodiments or elements thereof can occur or be performed simultaneously, at the same point in time, or concurrently.

[032] Reference is made to Fig. 1, showing a schematic block diagram of an exemplary computing device, according to embodiments of the present invention. Computing device 100 may include a controller 105 that may be, for example, a central processing unit processor (CPU), special purpose processor such as a graphic processing unit (GPU), communication control processing (CCP), a chip or any suitable computing or computational device, an operating system 115, a memory 120, a storage 130, an input devices 135 and an output device 140. Controller 105 may be configured to carry out methods as disclosed herein by for example executing code or software.

[033] Operating system 115 may be or may include any code segment designed and/or configured to perform tasks involving coordination, scheduling, arbitration, supervising, controlling or otherwise managing operation of computing device 100, for example, scheduling execution of programs. Operating system 115 may be a commercial operating system. Memory 120 may be or may include, for example, a Random Access Memory (RAM), a read only memory (ROM), a Dynamic RAM (DRAM), a Synchronous DRAM

(SD-RAM), a double data rate (DDR) memory chip, a Flash memory, a volatile memory, a non-volatile memory, a cache memory, a buffer, a short term memory unit, a long term memory unit, or other suitable memory units or storage units. Memory 120 may be or may include a plurality of, possibly different memory units.

[034] Executable code 125 may be any executable code, e.g., an application, a program, a process, automated task, software bots configured to manage data communication and user data collection (e.g., botnet), software adapted to perform artificial intelligence (AI), e.g. machine learning, deep learning, task or script. Executable code 125 may be executed by controller 105 possibly under control of operating system 115. Where applicable, executable code 125 may carry out operations described herein in real-time. Computing device 100 and executable code 125 may be configured to update, process and/or act upon information at the same rate the information, or a relevant event, are received. In some embodiments, more than one computing device 100 may be used. For example, a plurality of computing devices (in serial and/or parallel) that include components similar to those included in computing device 100 may be connected to a network and used as a system.

[035] Storage 130 may be or may include, for example, a hard disk drive, a universal serial bus (USB) device or other suitable removable and/or fixed storage unit. Content may be stored in storage 130 and may be loaded from storage 130 into memory 120 and may be stored in read only memory (ROM) to be loaded into memory 120 where it may be processed by controller 105. In some embodiments, some of the components shown in Fig. 1 may be omitted. For example, memory 120 may be a non-volatile memory having the storage capacity of storage 130. Accordingly, although shown as a separate component, storage 130 may be embedded or included in memory 120.

[036] Input devices 135 may be or may include a mouse, a keyboard, a touch screen or pad or any suitable input device. In some embodiments, computing device 100 receives input from a sensor such as global positioning system (GPS), camera, microphone, accelerometer, light sensor, compass, and any other sensor. It will be recognized that any suitable number of input devices may be operatively connected to computing device 100 as shown by block 135. Output devices 140 may include one or more displays, indicators, speakers, haptic output and/or any other suitable output devices. It will be recognized that any suitable number of output devices may be operatively connected to computing device 100 as shown by block 140. Any applicable input/output (I/O) devices may be connected

to computing device 100 as shown by blocks 135 and 140. For example, a wired or wireless network interface card (NIC), a modem, a universal serial bus (USB) device or external hard drive, cellular network connection, optical network connection, Bluetooth, and NFC may be included in input devices 135 and/or output devices 140.

[037] Embodiments of the invention may include an article such as a computer or processor non-transitory readable medium, or a computer or processor non-transitory storage medium, such as for example a memory, a disk drive, or a USB flash memory, encoding, including or storing instructions, e.g., computer-executable instructions, which, when executed by a processor or controller, carry out methods disclosed herein. For example, a storage medium such as memory 120, computer-executable instructions such as executable code 125 and a controller such as controller 105.

[038] Some embodiments may be provided in a computer program product that may include a non-transitory machine-readable medium, with instructions stored thereon, which may be used to program a computer, or other programmable devices, to perform methods as disclosed herein. Embodiments of the invention may include an article such as a computer or processor non-transitory readable medium, or a computer or processor non-transitory storage medium, such as for example a memory, a disk drive, or a USB flash memory, encoding, including or storing instructions, e.g., computer-executable instructions, which when executed by a processor or controller, carry out methods disclosed herein. The storage medium may include, but is not limited to, any type of disk including magneto-optical disks, semiconductor devices such as read-only memories (ROMs), random access memories (RAMs), such as a dynamic RAM (DRAM), erasable programmable read-only memories (EPROMs), flash memories, electrically erasable programmable read-only memories (EEPROMs), magnetic or optical cards, or any type of media suitable for storing electronic instructions, including programmable storage devices.

[039] A system according to embodiments of the invention may include components such as, but not limited to, a plurality of central processing units (CPU) or any other suitable multi-purpose or specific processors or controllers, a plurality of input units, a plurality of output units, a plurality of memory units, and a plurality of storage units. A system may additionally include other suitable hardware components and/or software components. In some embodiments, a system may include or may be, for example, a personal computer, a desktop computer, a mobile computer, a laptop computer, a notebook computer, a

terminal, a workstation, a server computer, a Personal Digital Assistant (PDA) device, a tablet computer, a network device, a smartphone, IOT device, action specific computerized machine (such as a dedicated robot) or any other suitable computing device. Unless explicitly stated, the method embodiments described herein are not constrained to a particular order or sequence. Additionally, some of the described method embodiments or elements thereof can occur or be performed at the same point in time.

[040] Reference is now made to Fig. 2, which schematically illustrates a data mapping system 200 for mapping of private data during communication with a remote server 201, according to some embodiments of the invention. The direction of arrows in Fig. 2 may indicate the direction of information flow. In order to manage private data for individual users, data mapping system 200 may initially map data types and data patterns (for example as a calibration process), as further described hereinafter. It should be noted that private data as used hereinafter may refer to any data and/or portion of data representing user's behavior, habits, characteristics, opinions, preferences, tendencies, relations, actions, status parameters (e.g., social, health, economic/wealth, legal, dependencies, being part of group and the like) and the like. In some embodiments, the user may be a computerized device (e.g., IOT, bot and the like) automatically operating on the user's behalf, so that the private data may refer to data and/or characteristics of the computerized device. Private data may also include privacy data and/or privacy preference(s).

[041] A user may choose based on private preference to share some private data and not to share other private data. Users may choose to share same private data with specific server and/or application and not to share it with different servers and/or application. In some embodiments, users may change such preference(s) at any applicable point in time. In some embodiments, private data may be automatically created to represent at least one feature of a computerized device and/or of the user of the computerized device. In some embodiments, private data may include at least one communication pattern and/or communication origin and destination and/or digital footprint and/or digital trace and/or digital response and/or digital reference. In some embodiments, private data may be received from analysis of data and/or from an external sensor and/or other source.

[042] The server 201 may be coupled to processor 202 such as controller 105, shown in Fig. 1. In some embodiments, processor 202 may receive at least one data packet 203 from server 201 to be mapped. For instance, processor 202 may receive at least one data packet

203 from a set of predetermined (or pre-classified) data packets 203. In some embodiments, processor 202 may receive from server 201 a request for sharing at least one data packet 203, for instance a request to share data packet with a contact name or contact directory data, where an automatic response may be created for each such request. It should be noted that data of such responses may also be considered as data packets 203 (e.g., to be mapped).

[043] In some embodiments, data mapping system 200 may include at least one data type database 204 and/or at least one data pattern database 205 and/or at least one privacy preference database 206 coupled to processor 202. In some embodiments, processor 202 may analyze the received data packet 203 to determine data type 207 of the data packet 203, for example by verifying at least one characteristic of the data packet 203. An examplary mapping of data types 207 is shown in Fig. 3A.

[044] In some embodiments, processor 202 may receive (e.g., from a user) privacy preference 209 to map the privacy preference database 206 for each data type and/or data pattern of the at least one data packet 203. In some embodiments, data mapping system 200 may include a modification algorithm 210, coupled to processor 202, and configured to, modify content of data packets according to at least one privacy preference 209 (e.g., nullify a content of a data packet). For example, the user may select a privacy preference 209 for forbidden sharing of location such that modification algorithm 210 may modify the content of the data packet 203 per a predetermined algorithm, for instance randomly modify the location (country) to any other country from a list of countries (e.g., Italy).

[045] Reference is now made to Fig. 3A, which schematically illustrates examplary mapping of data type database 204, according to some embodiments of the invention. Processor 202 may receive a request to share at least one data packet 203 (e.g., from server 201) and analyze characteristics of the at least one data packet 203, for example analyze characteristics of automatically created responses for the request. In some embodiments, the content of the received at least one data packet 203 may be analyzed for purposes of data type mapping.

[046] According to some embodiments, characteristics of the received at least one data packet 203 may be determined and dynamically fitted to an 'i'-dimensional vector 304 (e.g., static characteristics determined from metadata). It should be noted that while the characteristics vector 304 shown in Fig. 3A is five-dimensional, such vectors may have a

large number of characteristics. For example, an injective vector having dimensions of 50 characteristics (so that 'i'=50) or more. In some embodiments, an increased number of parameters in the characteristics vector 304 may improve chances of correctly determining the data type 207 until optimal determination of various data types may be achieved.

[047] At least one of the following characteristics of a data packet 203 may be injectively determined for each data packet: header, footer, version number, request by hostname/IP, sent to hostname/IP, server hostname/IP, IP address, file extension, , standard title, non-standard title, , encryption yes/no, encryption method, encoding yes/no, encoding method (e.g., 'UTF8'), whole file, chunked file, keywords, API version, SDK version, Social plug-in version, driver, communication protocol, action verbs, HTTP/HTTPS, URL Part Names, and/or any other specific character 'i' within the at least one data packet 203. The determined characteristics vector 304 may be associated with a particular data type 207 (since every data packet 203 corresponds to some data type 207), that may be still unknown (e.g., in terms of its content) and for instance indicated as data type 'j'. In some embodiments, processor 202 may receive at least one pre-classified data packet 203 with a known data type. In some embodiments, the data type 207 of characteristics vector 304 for the data-mapping stage, may be determined by reading the content of the corresponding data packet 203, for example reading content for the country name, web browsing history, operating system, etc.

[048] Such data types 207 (or characteristics vectors 304) that are gathered by processor 202, and possibly still having unknown data type content (e.g., data type 'j') at this stage, may be stored (e.g., stored in memory such as memory 120 shown in Fig. 1) at data type database 204 in order to carry out the data type mapping. Processor 202 may map the stored data types to link characteristics vectors 304 with data types 207. In some embodiments, processor 202 may determine that characteristics vectors 304 having at least one identical characteristic may correspond to a particular data type 207 (e.g. Web content search history type).

[049] Reference is now made back to Fig. 2. In some embodiments, data pattern database 205 may include at least one data pattern 208 corresponding to responses to sharing of at least one data packet 203. Similarly to mapping of data types (e.g., as shown in Fig. 3A), processor 202 may map data patterns of responses to request of sharing data packets 203. It should be noted that while the data type 207 of a data packet 203 may correspond to

static parameters (e.g., email address), the data patterns 208 may correspond to features of the dynamic data flow of data packet 203 that may be regarded as the "behavior" of the data packet 203.

[050] Reference is now made to Fig. 3B, which schematically illustrates examplary mapping of data pattern database 205, according to some embodiments of the invention. Processor 202 may receive at least one data packet 203 (e.g., from server 201), for example at least one response (or data packet) corresponding to a request for sharing the data packet 203 to analyze pattern behavior of the at least one response (or data packet). In some embodiments, the content of the received at least one data packet 203 may be analyzed to determine the data pattern. For example, at least one response may injectively correspond to a request for sharing at least one data packet 203 and/or a characteristic of the data packet 203 (e.g., a picture file from memory or from camera).

[051] It should be noted that while the pattern vector 305 shown in Fig. 3B is four-dimensional, such vectors may have a large number of features or ranges. For example, an injective vector 305 having dimensions of 100 features and/or ranges (so that 'm'=100) or more. At least one of the following dynamic features of a data pattern may be determined for each data packet: frequency (e.g., appearance(s) per second), size (e.g., in kilobytes), speed (in kilobytes per second), count (e.g., numbers), ratio (e.g., compared to other datatype flow), repeat (e.g., cyclic order), order, server reference (e.g., website reference such as "example.com/feature") and/or any combination thereof and/or other pattern behavior 'm' within the at least one data packet. In some embodiments, ranges for every feature (e.g., frequency) may be determined (e.g., lowest and highest frequency) as a feature of the data pattern 208. In some embodiments, a range may refer to non-discrete values (in contrast to discrete or static values in data type mapping, as shown in Fig. 3A), for instance a range defining number of website sub references (e.g., "example.com/sub-feature/sub-feature" with two sub references).

[052] The determined feature or pattern behavior vector 305 may be associated with a particular data pattern 208 (since every data packet 203 corresponds to some data pattern 208), that may be still unknown and for instance indicated as data pattern 208 'n'. In some embodiments, processor 202 may receive at least one pre-classified data packet 203 with a known data pattern.

[053] Such data patterns 208 that are gathered by processor 202, and possibly still having unknown data pattern 'n' at this stage, may be stored (e.g., stored in memory such as memory 120 shown in Fig. 1) at data pattern database 205 in order to carry out the data pattern mapping. Processor 202 may map the stored data patterns 'n' to link behavior vectors 305 with data patterns 208. In some embodiments, processor 202 may determine that pattern behavior vectors 305 having at least one identical characteristic and/or range may correspond to a data pattern 208 (e.g., same frequency range). In some embodiments, data patterns 208 may be determined according to logical conditions and/or ranges, for example for responses having frequency and size features in within predetermined thresholds.

[054] Reference is now made to Fig. 3C, which schematically illustrates examplary mapping of privacy preference table 306, according to some embodiments of the invention. Processor 202 may receive at least one data packet 203 (e.g., from server 201), for example at least one response (or data packet) corresponding to a request for sharing the data packet 203 to analyze type and pattern behavior of the at least one response (or data packet) to create data type database 204 and data pattern database 205 as described above. In some embodiments, processor 202 may receive (e.g., from a user) privacy preference database 206 to map the privacy preference table 306 for each data type (content) and/or data pattern of the at least one data packet 203. For example, the user may fill a privacy preference template (e.g., selecting to allow sharing of username) for different options of data types and/or data patterns to determine the privacy preference table 306. In case that some data packet is forbidden for sharing (e.g., contact data and/or a password), the content of that data packet may be, for example randomly, modified by predetermined modification algorithm 210 such that the modified content (e.g., nullified password or randomly replaced to a dummy contact name from a list) may be shared. In some embodiments, processor 202 may only check the data type such that no pattern is checked in order to determine the policy to apply, for example sharing of password data types may be completely forbidden so that data patterns are not checked. In some embodiments, processor 202 may detect an IoT device and only check the data pattern where the data type may not be checked. In some embodiments, processor 202 may only check the data pattern such that no data type is checked, for example checking frequency limit and modifying in accordance with the predefined limitations. In some embodiments,

repetition in at least one forbidden characteristic (e.g., forbidden frequency) may cause blocking of data sharing.

[055] Reference is now made back to Fig. 2. In some embodiments, privacy preference database 206 may include at least one privacy preference 209 such as a template to link privacy preferences for the determined data types 207 and/or data patterns 208 and/or modification algorithm 210. For example, privacy preference database 206 may include an un-populated matrix with data types 207 and/or data patterns 208 and/or modification algorithm 210 such that a user may choose which data types (content) 207 and/or data patterns 208 to share. In some embodiments, data mapping system 200 may include a modification algorithm 210, coupled to processor 202, and configured to manage sharing of at least one data packet 203 based on its data type 207 and/or data pattern 208 to comply with at least one privacy preference 209. The operation of the modification algorithm 210 is further described in Fig. 5, hereinafter.

[056] In some embodiments, data mapping system 200 (shown in Fig. 2) may be used as a system to determine collection of uncontrolled information from hardware equipment. Some manufacturers embed into their products, hidden agent(s) which transmits at least one hidden data packet. As may be apparent to one of ordinary skill in the art, such systems and methods may identify "back door" ability which may be part of the hardware core functionality and/or part of unit's embedded software. In some embodiments, by implementing the data mapping system 200 (shown in Fig. 2), unrecognized type and/or pattern of data packet may be determined, wherein the unrecognized type and/or pattern of data packet may be generated internally (in contrast to being requested by the server). Such data packet may be stored and further investigated for its origin and destination.

[057] Reference is now made to Fig. 4, which schematically illustrates a data management system 400 for dynamic management of private data during communication between a remote server 401 (such as server 201 in Fig. 2) and at least one user's device 411, according to some embodiments of the invention. The direction of arrows in Fig. 4 may indicate the direction of information flow. It should be noted that the at least one user's device 411 may be a computerized device such as computing device 100, shown in Fig. 1.

[058] In some embodiments, data management system 400 may include a data type database 404 (such as data type database 204 in Fig. 2), coupled to processor 402, such

that processor 402 may modify data packets (e.g., modify responses) to requests for retrieval of data packets 403 that are not compatible with data types from a data type database 404 and/or with data patterns from a data pattern database 405. In some embodiments, data management system 400 may further include a user interface 413 to issue an alert upon detection of a request for retrieval of data packets 403 that is not compatible with the privacy preference. In some embodiments, data packets 403 from the user's device 411 may be a response created as full or partial extraction(s) selected from the group consisting of any one of user's device files (permanent or temporary), user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory user's device static memory or the like.

[059] In some embodiments, data management system 400 may further include a user database 421 and/or a server database 431 for mapping of users and/or servers. Each user and/or user's device 411 using data management system 400 may be registered in user database 421 with corresponding privacy preference from privacy preference database 406, such that each user and/or user's device 411 may be linked to at least one privacy preference from privacy preference database 406. In some embodiments, server database 431 may include a list of servers 401 for communication with user devices 411. For example, a user may determine a predefine list of servers 401 for sharing of data (e.g., determine a whitelist). Thus, privacy preference database 406 may link privacy and/or sharing preferences for each user and/or server and/or data type and/or data pattern.

[060] In some embodiments, data management system 400 may perform at least one of sharing, blocking and/or modifying, per the modification algorithm 410 (e.g., such as modification algorithm 210, shown in Fig. 2), data packets 403 during communication between server 401 and user's device 411 according to the corresponding privacy preference from privacy preference database 406. For example, requests for sharing of data packets 403 of unrecognized data type may be blocked, requests for sharing of data packets 403 of allowed data type are shared, and requests for sharing of data packets 403 of forbidden data type are modified such that a predetermined response may be shared (e.g., nullify of contact data and randomly change to different mobile carrier from carrier list). In some embodiments, modification algorithm 410 may be configured for each mapped data type and/or data pattern so as to maintain communication as well as the

privacy preference by, for example randomly, modifying forbidden data packet (content) for sharing.

[061] In some embodiments, data mapping system 200 (shown in Fig. 2) may be continuously updates such that blocked unrecognized data types may be stored in a dedicated memory (such as memory 120 in Fig. 1) until this data type is mapped and recognized.

[062] In some embodiments, data management system 400 may perform at least one of sharing, blocking and modifying data packets 403 during communication between server 401 and user's device 411 in substantially real time such that the user may continue operation of user's device 411 while data management system 400 may operate in the background and/or operate in application mode for some operating systems (e.g., IOS) and/or some browsers (e.g., Safari). In some embodiments, data management system 400 (in contrast to the data-mapping stage) may handle encrypted data packets 403 since determination of data type does not read and concern the actual content of the data packet 403 even if the content is encrypted. It should be noted that while the mapping stage (e.g., described in Figs. 2 and 3A-3C) may require reading the content of the data packets for initial determination of data type and/or data pattern and/or privacy preference, the data management system 400, in contrast, does not need to read the actual content of the data packets.

[063] In some embodiments, data management system 400 may include a data pattern database 405 (such as data pattern database 205 in Fig. 2) with at least one data pattern corresponding to sharing of at least one data packet 403 (such as data packet 203 in Fig. 2) from user's device 411. In some embodiments, various data packets may be analyzed (e.g., by a processor) to determine reoccurring data patterns and thereby create data pattern database 405. As may be apparent to one of ordinary skill in the art, computerized devices such as user's device 411 may include a plurality of data packets 403 with various information (e.g., time zone, type of operating system, location, web browsing history, mouse movement, external audio, eye's focus tracking etc.) regarding the user's device 411.

[064] During communication with remote servers such as server 401, the server may send requests for sharing of these data packets 403, wherein the user's device 411 may automatically provide a corresponding response (or data packet) that is compatible with

the received request without knowledge, control and/or authorization of the user. According to some embodiments, data management system 400 may manage data packets 403 that are shared with server 401 according to a predefined privacy preference. In some embodiments, data management system 400 may further include a privacy preference database 406 (such as privacy preference database 206 in Fig. 2) with a predetermined privacy preference and/or a list of allowed and/or forbidden types of data packets 403 for sharing and/or modifying and/or, if not recognized, for blocking during communication with the at least one user's device 411. In some embodiments, at least some elements of the data management system 400 may be similar to corresponding elements in data mapping system 200, for example privacy preference database 406 while the content of data packet is not read.

[065] In some embodiments, data management system 400 may further include a communication module 412 configured to allow communication between the server 401 and the at least one user's device 411. In some embodiments, a user may determine at least one privacy preference from privacy preference database 406 with privacy preferences for data types and/or data patterns that the user allows for sharing (and/or forbidden types to be modified and/or, if not recognized types, to be blocked), for example the user may choose to block sharing of location data of any kind.

[066] In some embodiments, data management system 400 may further include a processor 402 (such as controller 105, shown in Fig. 1) coupled to the data pattern database 405 and to the privacy preference database 406. In some embodiments, processor 402 may be coupled to communication module 412. In some embodiments, processor 402 may be embedded in user's device 411. In some embodiments, processor 402 may determine at least one data pattern for sharing of data packet 403 that is for example compatible with the list of allowed types of data packets 403 from data type database 404 for sharing. In some embodiments, processor 402 may be embedded in server 401.

[067] In some embodiments, data management system 400 may operate in user's device 411 (e.g., in the form of internal proxy) to manage sharing of data packets 403, while data management system 400 may not affect other functionalities of the user's device 411 so as to allow uninterrupted usage of the device.

[068] Reference is now made to Fig. 5, which shows a flowchart for a method of management of data packets with a sharing algorithm during communication between a

remote server and a user's device, according to some embodiments of the invention. The processor (e.g., processor 402) may provide a data packet 403, for instance in response to a request for sharing of data. The received data packet 403 may be checked 501 for known or unknown element, for instance checked 501 for known data type and/or known data pattern based on data type database 404 and/or data pattern database 405. According to some embodiments, unknown elements may be determined as unrecognized and be blocked 510 by the sharing algorithm and not shared (e.g., with the server).

[069] In some embodiments, known elements may be checked 502 for allowed or forbidden elements, for instance checked 502 for allowed data type and/or allowed data pattern based on privacy preference database 406. According to some embodiments, allowed elements may be shared 520 by the sharing algorithm. According to some embodiments, forbidden elements may be, for example randomly, modified 530 by the predetermined modification algorithm 410 with sharing 520 of the modified content (e.g., with the server). For example, a user choosing not to share the country name may choose a privacy preference to modify such data packet to always share a random country name from a list of countries (e.g., "France") by modifying the data packet to be shared with the user, in order to maintain ongoing communication with the server.

[070] It should be noted that with data management system 400, the user may choose features for sharing such that other features that are forbidden for sharing may be modified so as to allow continuous and uninterrupted communication with the server.

[071] Reference is now made to Fig. 6A, which shows a flowchart for a method of dynamic management of private data during communication between a remote server 401 and a user's device 411, according to some embodiments of the invention. In some embodiments, user's device 411 may receive 601 a request for retrieval of at least one data packet 403 from the user's device 411, wherein the user's device 411 may provide a response corresponding to the received request.

[072] In some embodiments, the user's device 411 may determine 602 the data type of the at least one data packet 403 corresponding to the received request. In some embodiments, the user's device 411 may receive 603 a privacy preference for the user's device 411, wherein the privacy preference includes a list of allowed (or forbidden) data packet types for sharing (or randomly modifying per the predetermined modification algorithm for each forbidden data type) during communication. In some embodiments,

data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference may be modified 604. In some embodiments, responses to requests for sharing of data packets 403 of unrecognized type may be blocked. In some embodiments, communication between the remote server 401 and the user's device 411 may be maintained 605 with sharing of the modified data packets (e.g., responses).

[073] In some embodiments, the user's device 411 may determine a pattern of at least one response corresponding to the received request, and modify data packets (e.g., responses) to requests for sharing of data packets 403 corresponding to at least one data pattern that are not compatible with the received privacy preference. In some embodiments, the privacy preference may include a list of allowed data patterns for sharing during communication.

[074] It should be noted that such predetermined modification per each forbidden data packet type, may be a fixed or random action, depend on the user's preference and the content (e.g. nullify for password and randomly change to different country from countries list). For data packets that are not compatible with the received privacy preference (as determined by the user) may allow users to optimally control sharing of their data. For example, a user choosing not to share location data may use the system to randomly modify the data packets during communication (as above) such that the location data may not be transferred via other means (e.g., user's instruction not to share location, application blocking only sensor GPS data while sharing country code data).

[075] In some embodiments, the user's device 411 may include a database with at least one data packet type corresponding to a request for sharing of data packets 403 from the user's device 411, wherein the type of data packets 403 may be determined from the data packet type database. In some embodiments, at least one response may be linked to a type of data packet 403 from the user's device 411, wherein the linking may be based on the data type and data pattern of the at least one response.

[076] In some embodiments, a response corresponding to a request for sharing of data packets may be identified (e.g., by a processor 402), wherein the identified response is not compatible with the received privacy preference. In some embodiments, a response with at least one modified data packet corresponding to the request for sharing types of data packets may be provided per the modification algorithm. In some embodiments,

modification of the at least one modified data packet 403 may be selected from the group consisting of data nullification, change of encoding and/or file template, change of header and/or footer, blocking, data randomization, content modification, addition of a predetermined data packet, encryption or the like.

[077] In some embodiments, a communication pattern between the server 401 and the user's device 411 may be identified, wherein the communication pattern may include at least one request for retrieval of at least one data packet 403 from the user's device 411 and corresponding responses. In some embodiments, an alert may be issued (e.g., by a processor 402) upon detection of a change in the identified communication pattern. In some embodiments, data packets 403 from the user's device 411 may be a response created as full or partial extraction(s) selected from the group consisting of any one of user's device files (permanent or temporary), user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory user's device static memory or the like. .

[078] Reference is now made to Fig. 6B, which shows a flowchart for a method of dynamic management of private data during communication between a remote server 401 and a user's device 411, according to some embodiments of the invention. In some embodiments, user's device 411 may receive 611 a request for retrieval of at least one data packet 403 from the user's device 411, wherein the user's device 411 may provide a response corresponding to the received request.

[079] In some embodiments, user's device 411 may determine 612 at least one data pattern corresponding to the received request. In some embodiments, user's device 411 may receive 613 a privacy preference for the user's device 411, wherein the privacy preference may include a list of allowed (and/or forbidden) data patterns for sharing (and/or randomly modifying according to the predetermined modification algorithm for each of the forbidden data patterns) during communication. In some embodiments, responses corresponding to requests for sharing of data packets and corresponding data patterns that are not compatible with the received privacy preference may be modified 614. In some embodiments, communication between the remote server 401 and the user's device 411 may be maintained 615 with sharing of the modified responses.

[080] In some embodiments, user's device 411 may determine the type of the at least one data packet 403 of the received request. In some embodiments, requests for sharing of data

packets 403 and corresponding data patterns, corresponding to at least one data packet type, that are not compatible with the received privacy preference may be modified. In some embodiments, the privacy preference may include a list of allowed (and/or forbidden) data packet types for sharing (and/or modifying) during communication.

[081] In some embodiments, user's device 411 may include a database with at least one data pattern corresponding to a request for sharing of data packets from the user's device, and wherein the at least one data pattern compatible with the received request may be determined from the database. In some embodiments, user's device 411 may determine the type of the at least one data packet 403 of the received request, and link at least one data pattern to a type of data packet from the user's device 411, wherein the linking may be based on the pattern of the at least one response.

[082] In some embodiments, a data pattern corresponding to a request for sharing of types data packets 403 may be identified (e.g., by a processor 402), wherein the identified data pattern is not compatible with the received privacy preference. In some embodiments, a response with at least one modified data packet corresponding to the request for sharing types of data packets may be provided.

[083] In some embodiments, an alert may be issued (e.g., by a processor 402) upon detection of a request for sharing data packets, wherein the detected request does not correspond to a data type and/or a data pattern and/or a combination thereof that is not compatible with the received privacy preference. In some embodiments, a communication pattern between the server 401 and the user's device 411 may be identified, wherein the communication pattern may include at least one request for retrieval of at least one data packet 403 from the user's device 411 and corresponding responses. In some embodiments, an alert may be issued (e.g., by a processor 402) upon detection of a change in the identified communication pattern.

[084] In some embodiments, a data management system (e.g., data management system 400 as shown in Fig. 4) may be implemented as an exit gatekeeper to monitor outflow communication. For example, in network embedded devices (NED) with limited CPU power, low memory capacity and low power resources means (e.g., internet of things (IOT) device and/or machine to machine and/or machine to server communication and/or other thin client or the like). Outflow communication may be monitored for communication patterns and/or data packet type and/or data pattern and once going out of

predefined type and/or pattern range, may limit communication flow and/or block it. This ability to monitor and control outflow communication by the system may prevent for any user's device and/or NED, from being part of communication overloading attacks for example distributed denial of service (DDoS) attack or the like. Such attacks may be created by malicious attackers who are remotely using uncontrolled user's device and/or NED or the like, to generate very high communication flow (e.g., 1 terabyte per second) in short period of time (e.g. hundreds of thousands or more of IP address endpoints at the same time) that basically overload the attacked server(s) until it adversely impacts its ability to function and in some cases creates fatal malfunction in mission critical systems.

[085] Reference is now made to Fig. 7, which schematically illustrates a data management system 700 for dynamic management of private data that is at least partially embedded on a hardware component 711 (indicated with a solid line), according to some embodiments of the invention. The data management system 700 may include the communication module and/or processor adjusted and preconfigured to privacy preference methods and processes and/or data storage such as privacy preference database. The data management system 700 may be at least partially embedded on a hardware component 711, for instance embedded on one chip and/or integrated circuit and/or processor. According to some embodiments the system may communicate with server 401 and/or user's device 411 via the communication module 412. In some embodiments, the hardware component 711 (indicated with a solid line) may include at least one privacy preference database that been preconfigured and may be updated only locally so that no remote change can be made, for example by using electrically erasable programmable read-only memories (EEPROMs). In some embodiments, the hardware component 711 (indicated with a solid line) may be embedded and/or added to user's device 411 (indicated with a dashed line).

[086] For example, such data management system 700 may be added into an IOT device (e.g., adding a chip and/or a circuit to the CPU) such that DDoS may be prevented, for example, communication between the IOT device may be monitored and controlled for unusual communication patterns, such that data patterns containing higher frequency (e.g. higher than ten data packets per second) and/or data flow (e.g., higher than 1megabyte per second) may be blocked by the system, according to privacy preferences determined for that purpose. For example, as shown in Fig. 3C as well. It should be noted that such

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number:		**PCT/IL2018/050359**
International filing date:		**28 March 2018 (28.03.2018)**
Document type:		**Certified copy of priority document**
Document details:	Country/Office:	**IL**
	Number:	**251683**
	Filing date:	**09 April 2017 (09.04.2017)**
Date of receipt at the International Bureau:		**15 April 2018 (15.04.2018)**

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-*bis*)

34, chemin des Colombettes
1211 Geneva 20, Switzerland
www.wipo.int

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2018 (18.10.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/189736 A1

(51) International Patent Classification:
H04L 29/12 (2006.01)

(21) International Application Number:
PCT/IL2018/050359

(22) International Filing Date:
28 March 2018 (28.03.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
251683 09 April 2017 (09.04.2017) IL

(72) Inventor; and
(71) Applicant: **KOREN, Yoseph** [IL/IL]; 91/33 Hagalil street, 5591491 Ganey-Tikva (IL).

(72) Inventor: **WASSERMAN, Yehonatan**; 39 Kaplan St., 5529339 Kiryat-Ono (IL).

(74) Agent: **FRYDMAN, Idan** et al.; Pearl Cohen Zedek Latzer Baratz, P.O. Box 7198, 6107121 Tel Aviv (IL).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, 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:
— *with international search report (Art. 21(3))*

(54) **Title:** SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

(57) **Abstract:** Systems and methods of dynamic management of private data during communication between a remote server and a user's device, including receipt of a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request, determination of at least one communication data type of the at least one data packet correspondin g to the received request, receipt of a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication, modification of data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference and maintenance of communication between the remote server and the user's device, with sharing of the modified data packet.

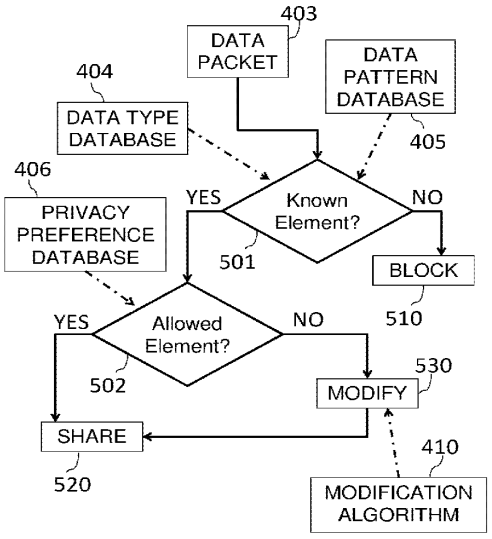


Fig. 5

WO 2018/189736 A1

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92*bis*.1 and Administrative Instructions, Section 422)

To:

FRYDMAN, Idan
Pearl Cohen Zedek Latzer Baratz
P.O. Box 7198
6107121 Tel Aviv
ISRAËL

Date of mailing *(day/month/year)*
24 April 2018 (24.04.2018)

Applicant's or agent's file reference
P-566702-PC

IMPORTANT NOTIFICATION

International application No.
PCT/IL2018/050359

International filing date *(day/month/year)*
28 March 2018 (28.03.2018)

1. The following indications appeared on record concerning:

☒ the applicant ☐ the inventor ☐ the agent ☐ the common representative

Name and Address

KOREN, Yoseph
91/33 Hagalil street
5591491 Ganey-Tikva
Israel

State of Nationality: IL
State of Residence: IL
Telephone No.
Facsimile No.
E-mail address

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☐ the name ☐ the address ☐ the nationality ☐ the residence

Name and Address

See box 3.

State of Nationality
State of Residence
Telephone No.
Facsimile No.
E-mail address
☐ Notifications by e-mail authorized

3. Further observations, if necessary:
Mr. Yoseph Koren is now recorded as applicant and inventor for all designated States.

4. A copy of this notification has been sent to:

☒ the receiving Office
☐ the International Searching Authority
☐ the Authority(ies) specified for supplementary search
☐ the International Preliminary Examining Authority
☐ the designated Offices concerned
☐ the elected Offices concerned
☒ other: KOREN, Yoseph

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 71 30

Authorized officer
Fahy Laurence
e-mail pct.team9@wipo.int
Telephone No. +41 22 338 74 09

REQUEST FOR PARTICIPATION IN THE GLOBAL/IP5 PATENT PROSECUTION HIGHWAY (PPH) PILOT PROGRAM IN THE USPTO

Application No.:	Not yet assigned	First Named Inventor:	Yoseph KOREN
Filing Date:	Herewith	Attorney Docket No.:	P-566702-US
Title of the Invention:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA		

THIS REQUEST FOR PARTICIPATION IN THE PPH PILOT PROGRAM ALONG WITH THE REQUIRED DOCUMENTS MUST BE SUBMITTED VIA EFS-WEB. INFORMATION REGARDING EFS-WEB IS AVAILABLE AT
https://www.uspto.gov/patents-application-process/applying-online/about-efs-web

APPLICANT HEREBY REQUESTS PARTICIPATION IN THE PATENT PROSECUTION HIGHWAY (PPH) PILOT PROGRAM AND PETITIONS TO MAKE THE ABOVE-IDENTIFIED APPLICATION SPECIAL UNDER THE PPH PILOT PROGRAM.

Office of earlier examination (OEE): Israel (Israeli Patent Office)

OEE application number: IL 251683

Both the OEE application and the above-identified U.S. application have the following earliest date (filing or priority date): April 9th, 2017

Type of OEE work product relied upon: Decision to grant a patent

Mailing date of OEE work product: May 16th, 2019

Supporting Documents

1. OEE Work Product and Translation

A copy of the OEE work product and translation if not already in English:

☒ Attached ☐ Previously Submitted ☐ Not required because the decision to grant a patent was the first office action

☐ Applicant requests the USPTO to attempt to obtain the OEE work productd from the Dossier Access System or PATENTSCOPE

NOTE: If the applicant requests the USPTO to obtain the OEE work product electronically and such attempt is unsuccessful, the applicant will be required to supply the document. Accordingly, to avoid dismissal of the initial PPH request and potential denial of participation in the PPH program, the applicant should verify that the OEE work product is actually available via the Dossier Access System or PATENTSCOPE before requesting retrieval. If the applicant is unable to verify availability, then the applicant should submit the document with the PPH request.

2. References Cited in OEE Work Product

An information disclosure statement (IDS) listing the references cited in the OEE work product and document copies (except U.S. patents and U.S. published patent applications):

☒ Attached ☐ Previously Submitted ☐ Not required because no references were cited in the OEE work product

This collection of information is required by 35 U.S.C. 119, 37 CFR 1.55, and 37 CFR 1.102(d). 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 2 hours 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

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.

REQUEST FOR PARTICIPATION IN THE GLOBAL/IP5 PPH PILOT PROGRAM IN THE USPTO
(continued)

Application No.:	Not yet assigned	First Named Inventor:	Yoseph KOREN

3. Claims Correspondence Certification Statement

All of the claims in this application sufficiently correspond to the patentable/allowable claims in the OEE application.

4. Claims Correspondence Table

Claims in U.S. Application	Patentable Claims in OEE Application	Explanation Regarding the Correspondence
1	1	Amended to be identical
2	2	Identical
3	3	Identical
4	4	Amended to be identical
5	5	Identical
7	7	Identical
8	8	Identical
9	9	Identical
12	12	Amended to be identical
13	13	Identical
14	14	Identical
15	15	Amended to be identical
17	17	Identical
18	18	Identical
19	19	Identical
20	20	Identical
24	24	Amended to be identical
26	26	Identical
27	27	Identical
28	28	Identical

Signature	/Devorah N. Livneh, Reg. No. 71,347/	Date	October 7, 2019
Name (print or type)	Devorah N. Livneh	Registration Number	71,347

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.

[emblem]
State of Israel
Ministry of Justice

[logo]
Patent Office

PK 13

Date: 11 Iyar 5779
May 16, 2019
Your number: P-566702-IL

Pearl Cohen Zedek Latzer Baratz
Azrieli Sarona Tower, 121 Menachem Begin Rd. 121 53rd floor Tel Aviv PO Box 7198
Israel 6107121

Ladies and gentlemen:

Subject: **Notice before filing of Patent Application number 251683**

Reference: Your letter dated November 29, 2018

Please note: Where reference is made to a law, this means the Patents Law, 5727-1967. Where reference is made to regulations, this means the Patents Regulations (Office Practice, Rules of Procedure, Documents and Fees), 5728-1968. In accordance with the Registrar's Circular 035/2017 – Patents, **publication of patent applications may not be delayed pursuant to Section 26 of the Law.**

This Notice is based on the following documents:
Claims dated: November 29, 2018
Specifications of the application dated: April 9, 2017
Drawings dated: April 9, 2017

Response to the Applicant's arguments
The Applicant has limited Independent Claim 1 and has explained why the publications cited do not preclude the claim. The explanation is acceptable and the search did not find any other relevant publications. Therefore, the application is acceptable.
The examination of the application was accelerated in accordance with the provisions of Section 19a(a) of the Law.

I hereby inform you that the examination of the above-cited application has been completed pursuant to the provisions of Section 17(a)(1) and (2) of the Law.
The Applicant has limited Independent Claim 1 and has explained why the publications cited do not preclude the claim. The explanation is acceptable and the search did not find any other relevant publications. Therefore, the application is acceptable.

Payment of filing fees
1. The application will be accepted in accordance with Section 16 of the Law after payment of the filing fees.
2. The amount of the fee as of the date of this Notice is NIS 713.00. The sum is subject to revision based on the Index in accordance with Regulation 6a.
3. The fee must be paid within 3 months of the date of this Notice.
4. Subject to the following two conditions and in accordance with Item 10 in the second Supplement to the Patent Regulations the filing fee shall be reduced (40% discount) if:
    4.1 The application is the first application submitted for that invention, i.e. an application in Israel without any priority.
    4.2 The applicant meets one of the following definitions:
        4.2.1 The applicant is not a company or partnership

4.2.2 The applicant is a company or partnership that submits an affidavit to the effect that its turnover was no greater than NIS 10 million in the previous year.
4.2.3 The applicant is a recognized institution of higher education.

Formal review

The application will undergo a formal review shortly after this Notice before its publication and changes to it may be requested. If so, a notice from the examiner concerning the changes demanded will be received. The notice concerning the changes demanded will not void this Notice.
Attached to the present notice please find:
- a copy of the updated specifications of the application -- if there are any errors please notify the Office of them before the date of payment of the filing fee.
- a "Status of Patent Application" form -- for the purpose of authenticating the details of the publication in accordance with Section 26 of the Law. Please note that the bibliographical information appearing on the attached form constitute a part of the patent's specifications intended for publication on the Office's site.

Updating the list of citations and publications pursuant to Section 18a of the Law

Please note, in accordance with Registrar's Circular M.N. 31 updates to the list of citations and/or publications that are received in accordance with the requirement of Section 18a of the Law after the date of this Notice shall be retained in the Office's operating system and shall not be transmitted to the examiner for re-examination.

Submission of requests for division

In accordance with the provisions of Section 24(a) of the Law, until the application has been accepted, the Applicant is entitled to request the division of the application into individual applications. Therefore, if you wish to submit requests for division from this application you must do so before the filing date. We cannot recognize requests submitted after the filing date of the present application as requests for division with respect to Section 24(c) of the Law.

Delaying publication of the filing of the application

If the application has not yet been published pursuant to Section 16(a) of the Law, and you wish not to have the filing of the application published until 18 months from the date of submission of the application or from the date of submission of a priority application (whichever is earlier), you must notify the examiner of the application (the undersigned) of this promptly.

You may review the "Status of Patent Application" form using this link:
http://www.ilpatsearch.justice.gov.il/UI/reportviewer.aspx?reqNo=251683

You may review the details of the application file on the Office's site using this link:
http://www.ilpatsearch.justice.gov.il/UI/RequestDetails.aspx?ReqId=251683

Agudat Sport Hapoel St. 1, Malcha Technology Park
Building no. 5 Jerusalem 9695101
Tel: 972-2-5651666 Fax: 972-2-5651641
www.patents.gov.il

Sincerely yours,

[signature]

Noam Markowitz
Senior Examiner
Tel.: 02-5651735
Email: noamm@justice.gov.il
Team head: Ronen Lahav

פ.ק 13

תאריך : י"א אייר תשע"ט
16/05/2019
מספרכם : P-566702-IL

לכבוד
פרל כהן צדק לצר ברץ
מגדל עזריאלי- שרונה דרך מנחם בגין 121 קומה 53 תל-אביב ת.ד. 7198
ישראל 6107121

א. ג. נ.,

הנדון : **הודעה לפני קיבול בקשת פטנט מספר 251683**

סימוכין : מכתבכם מיום 29/11/2018

לתשומת לבכם: מקום בו הנכם מופנים לחוק, הכוונה היא לחוק הפטנטים, התשכ"ז – 1967. מקום בו הנכם מופנים לתקנות, הכוונה היא לתקנות הפטנטים (נוהלי הרשות, סדרי דין, מסמכים ואגרות), התשכ"ח – 1968. בהתאם לחוזר רשם 035/2017 – פטנטים **לא ניתן להשהות פרסום בקשות פטנט לפי סעיף 26 לחוק.**

הודעה זו מבוססת על המסמכים הבאים:

תביעות מתאריך : 29/11/2018
פרטי הבקשה מתאריך : 09/04/2017
שרטוטים מתאריך : 09/04/2017

מענה לטיעוני המבקש

המבקש צמצם את התביעה הבלתי תלויה 1 ונימק מדוע הפרסומים שצוטטו אינם מתגברים על התביעה. הנימוק מתקבל ובחיפוש לא נמצאו פרסומים אחרים רלוונטיים. על כן, הבקשה מתקבלת.

בחינת הבקשה הוקדמה בהתאם להוראות סעיף 19א(א) לחוק.

הריני להודיעכם כי בחינת הבקשה הנ"ל הושלמה לפי הוראות סעיף 17(א)(1) ו- (2) לחוק.

המבקש צמצם את התביעה הבלתי תלויה 1 ונימק מדוע הפרסומים שצוטטו אינם מתגברים על התביעה. הנימוק מתקבל ובחיפוש לא נמצאו פרסומים אחרים רלוונטיים. על כן, הבקשה מתקבלת.

תשלום אגרת קיבול

1. הבקשה תתקבל בהתאם לסעיף 26 לחוק לאחר תשלום אגרת הקיבול.
2. סכום האגרה נכון למועד הודעה זו הינו 713.00 ש"ח. הסכום כפוף לעדכונו על פי המדד בהתאם לתקנה 6א.
3. יש לשלם את האגרה תוך 3 חודשים מתאריך הודעה זו.
4. בכפוף לשני התנאים הבאים ובהתאם לפריט 10 בתוספת השנייה לתקנות הפטנטים תשולם אגרת קיבול מופחתת (40% הנחה) כאשר:
   4.1. הבקשה הינה הבקשה הראשונה המוגשת בגין אותה אמצאה, דהיינו, בקשה בישראל ללא דין קדימה.
   4.2. המבקש עונה לאחת מההגדרות הבאות:
      4.2.1. המבקש אינו חברה או שותפות.

4.2.2. המבקש הוא חברה או שותפות שהגישה תצהיר שמחזור עסקיה לא עלה על 10 מיליון ש"ח בשנה הקודמת.

4.2.3. המבקש הינו מוסד מוכר להשכלה גבוהה.

בדיקה פורמלית

הבקשה תעבור בדיקה פורמלית בסמוך להודעה זו לקראת פרסומה וייתכן שיתבקשו בה שינויים. באם כן, תתקבל הודעה מהבוחן לגבי השינויים הדרושים. ההודעה לגבי השינויים הדרושים לא תבטל הודעה זו.

להודעה הנוכחית מצורפים:

- העתק פירוט הבקשה המעודכן - אם נפלו טעויות נא להודיע עליהן לרשות לפני מועד תשלום אגרת הקיבול.
- טופס 'מצב בקשת פטנט' - לצורך אימות פרטי הפרסום בהתאם לסעיף 26 לחוק. שימו לב שהפרטים הביבליוגרפיים שמופיעים בטופס המצ"ב מהווים חלק מפירוט הבקשה המיועד לפרסום באתר הרשות.

עדכון רשימות האסמכתאות והפרסומים לפי סעיף 18א לחוק

לתשומת לבכם, בהתאם לחוזר רשם מ.נ. 31 עדכונים לרשימת האסמכתאות ו/או הפרסומים שיתקבלו בהתאם לדרישת סעיף 18א לחוק, לאחר תאריך הודעה זו ישמרו במערכת התפעולית שברשות ולא יועברו לבוחן לבחינה חוזרת.

הגשת בקשות חלוקה

בהתאם להוראות סעיף 24(א) לחוק זכאי המבקש כל עוד לא קובלה הבקשה לדרוש את חלוקת הבקשה לבקשות אחדות. לפיכך, באם ברצונכם להגיש בקשות חלוקה מבקשה זו עליכם לעשות זאת בטרם מועד הקיבול. לא נוכל להכיר בבקשות שיוגשו לאחר מועד הקיבול של הבקשה הנוכחית כבקשות חלוקה לעניין סעיף 24(ג) לחוק.

השהיית פרסום קיבול הבקשה

באם הבקשה עדיין לא פורסמה לפי סעיף 16(א) לחוק, והנכם מעוניינים שדבר קיבול הבקשה לא יתפרסם עד חלוף 18 חודש מיום הגשת הבקשה או מיום הגשת בקשת דין הקדימה (לפי המוקדם יותר), עליכם להודיע על כך לבוחן הבקשה (החתום מטה) בהקדם.

ניתן לעיין בטופס "מצב בקשת פטנט" באתר הרשות בקישור:

http://www.ilpatsearch.justice.gov.il/UI/reportviewer.aspx?reqNo=251683

ניתן לעיין בפרטי תיק הבקשה באתר הרשות בקישור:

http://www.ilpatsearch.justice.gov.il/UI/RequestDetails.aspx?ReqId=251683

בכבוד רב



נעם מרקוביץ
בוחן פטנטים בכיר
טלפון: 073-3927224
דואר אלקטרוני: noamm@justice.gov.il
ראש צוות: רונן להב

[emblem]
State of Israel
Ministry of Justice

[logo]
Patent Office

PK 26

Date: 19 Av 5778
July 31, 2018
Your number: P-566702-IL

Pearl Cohen Zedek Latzer Baratz
Azrieli Sarona Tower, 121 Menachem Begin Rd. 121 53rd floor Tel Aviv PO Box 7198
Israel 6107121

Ladies and gentlemen:

Subject: **Notice of deficiencies in Patent Application no. 251683**
Reference: Your letter dated January 21, 2018

Please note: Where reference is made to a law, this means the Patents Law, 5727-1967. Where reference is made to regulations, this means the Patents Regulations (Office Practice, Rules of Procedure, Documents and Fees), 5728-1968. You must respond to this notice within four months of its date, but you may request an extension; with any request for extension submitted, you must pay a fee in the amount of NIS 201.00 for each month or part thereof. **No more than four months' extension shall be granted for each notice of deficiencies and the total of all the extension periods over the course of the examination shall not exceed 12 months** in accordance with the rules set forth in the Registrar's Circular 035/2017 - Patents.

This Notice is based on the following documents:
Drawings dated: April 9, 2017
Specifications of the application dated: April 9, 2017
Claims dated: January 21, 2018

The references in this notice refer to the following publications:
D1: WO2013103782 [3M INNOVATIVE PROPERTIES CO [US]; LAYSON HOYT M [US]] - 11/07/2013

Response to the Applicant's arguments

In accordance with that stated below in this Notice, the following is a summary of my position with regard to the patentability of the claims:
Deficiencies were found in Claims 1-28.
See the grounds below in this Notice.

In accordance with the provisions of **Regulation 43**, I wish to inform you that the following deficiencies were found in the above-cited application:

1. **Novelty and inventive step**
   1.1 Claims 1-2, 13 do not define a novel invention as defined in **Section 4 of the Law**, in light of Publication(s): D1

Regarding claim 1, D1 discloses a method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request (see ¶ 78, 232);
determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request (see ¶ 221, 494) ;
receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication (see ¶ 149, 221)
modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference (see ¶ 804) ; and
maintaining communication between the remote server and the user's device,with sharing of the modified data packets (see ¶ 804)

Therefore Claim(s) 1-2, 13 lack novelty.

1.2 Claim(s) 3-12, 14-28 do not define a new invention that includes an inventive step as defined in **Section 5 of the Law**, in light of what stated in Publication D1 in conjunction with the general knowledge of a person skilled in the art.

Regarding claims 3-12, 14-28, Skilled person would consider as obvious possibility to improve the data security by monitoring the packets traffic for detecting an abnormal traffic pattern, as suggested by those claims. Said traffic monitoring would not involve any surprising effect in respect to the problem of privacy protection, nor would it supplement special contribution in respect to the solution which recited by independent claim 1 and disclosed in D1, namely, inspecting packets content according to the user privacy preferences. It is pointed out that the examples which given in the supporting disclosure in relation to the 'pattern' monitoring are concerning with cyber threats, such as denial of service attacks, and not actually with the specific problem of protecting the user privacy. Thereby, it could be argus that employing the user privacy preferences in respect to the monitoring of the traffic pattern would not have any special advantage.

Therefore Claim(s) 3-12, 14-128 lack an inventive step.

2. The claims

2.1 Claims no. 1 do not comply with the provisions of **Section 13(a) of the Law** since they do not reasonably stem from that described in the specifications:

Claim 1 is not properly supported by the specifications, contrary to article 5. Said claim recites that the communication data type is determined by a remote server, whereas the disclosure describes that said determination is performed by the user device.

Therefore, the specifications of the application do not include references to the entire scope of the above-cited claims. You must provide grounds for the references in the specifications of the application for the above-cited claims as defined, or amend the definition of the claimed scope in accordance with the references in the specification.

Agudat Sport Hapoel St. 1, Malcha Technology Park
Building no. 5 Jerusalem 9695101
Tel: 972-2-5651666 Fax: 972-2-5651641
www.patents.gov.il

The Applicant's duty to update the Office

Your attention is drawn to **Section 18a of the Law** with respect to the Applicant's duty to update the Office concerning any change in the list of citations or publications as stated in **Section 18(a) of the Law,** and to **Section 18c** of the Law with respect to means of enforcement.

Submission of amendments to the specifications during the examination of the application

If amendments are made to the patent application, your attention is drawn to **Regulation 22(a).** You must send the Office a complete copy of the part of the application in which the changes were made, and they must be clearly marked. An addition is to be marked by underlining (thus: example) and deletions crossed out (thus: ~~example~~). **Do not resubmit files that were not amended.**

Please note:

a) In accordance with Regulations 22(b) and 42, if you amend the specifications in order to remedy the deficiencies in this notice, you must specify the deficiencies that the amendments are intended to remedy and explain how amending the specification corrects the deficiency.

b) In accordance with the provisions of the Registrar's Circular 034/2017- Patents, if the examination of the application began after March 27, 2017, amending the specification by replacing the invention that was examined and for which a deficiency was cited with another invention, whether it appeared in the claims originally or was only described, even if it stems from the description, does not constitute an amendment of the deficiency and shall result in the sending of a notice before denial.

Appeal to the Registrar

In accordance with **Section 161 of the Law**, you may appeal my decision to the Patents Registrar within four months of the date the notice was sent.

You may review the details of the application file on the Office's site using this link:
http://www.ilpatsearch.justice.gov.il/UI/RequestDetails.aspx?ReqId=251683

Sincerely yours,

[signature]

Noam Markowitz
Senior Examiner
Tel.: 02-5651735
Email: noamm@justice.gov.il
Team head: Ronen Lahav

תאריך : י״ט אב תשע״ח
31/07/2018
מספרכם : P-566702-IL

לכבוד
פרל כהן צדק לצר ברץ
מגדל עזריאלי- שרונה דרך מנחם בגין 121 קומה 53 תל-אביב ת.ד. 7198
ישראל 6107121

א. ג. נ.,

הנדון : **<u>הודעה על ליקויים בבקשת פטנט מספר 251683</u>**

סימוכין : מכתבכם מיום 21/01/2018

לתשומת לבכם: מקום בו הנכם מופנים לחוק, הכוונה היא לחוק הפטנטים, התשכ״ז – 1967. מקום בו הנכם מופנים לתקנות, הכוונה היא לתקנות הפטנטים (נוהלי הרשות, סדרי דין, מסמכים ואגרות), התשכ״ח – 1968. עליכם להשיב על הודעה זו תוך ארבעה חודשים מתאריכה, אך הנכם רשאים לבקש את הארכת התקופה, עם בקשת הארכה שתוגש יש לשלם אגרה בסך 201.00 ש״ח בעד כל חודש או חלק ממנו. **לא יינתנו יותר מארבעה חודשי ארכה בגין כל הודעה על ליקויים וסך כל תקופות הארכה במהלך הבחינה לא יעלה על 12 חודשים** בהתאם לכללים שנקבעו בחוזר הרשם 035/2017-פטנטים.

<u>הודעה זו מבוססת על המסמכים הבאים:</u>

שרטוטים מתאריך : 09/04/2017
פרטי הבקשה מתאריך : 09/04/2017
תביעות מתאריך : 21/01/2018

<u>ההפניות בהודעה זו מתייחסות לפרסומים הבאים:</u>

D1: WO2013103782 [3M INNOVATIVE PROPERTIES CO [US]; LAYSON HOYT M [US]] - 11/07/2013

<u>מענה לטיעוני המבקש</u>

.

<u>בהתאם למפורט בהמשך הודעה זו להלן סיכום עמדתי לעניין כשירות התביעות לפטנט:</u>
בתביעה/ות מס׳ 1-28 נמצאו ליקויים.
ראה הנימוקים בהמשך הודעה זו.

<u>בהתאם להוראות **תקנה 43** הנני להודיעכם כי נמצאו בבקשה הנ״ל הליקויים המפורטים להלן:</u>

1. <u>חידוש והתקדמות המצאתית</u>

1.1 תביעות 1-2,13 אינן מגדירות אמצאה חדשה כהגדרתה ב**סעיף 4 לחוק**, לאור פרסום/ים : D1.

Regarding claim 1, D1 discloses a method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request (see ¶ 78, 232);
determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request (see ¶ 221, 494) ;
receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication (see ¶ 149, 221)
modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference (see ¶ 804) ; and
maintaining communication between the remote server and the user's device,with sharing of the modified data packets (see ¶ 804)

לפיכך תביעה/ות 1-2,13 חסרות חידוש.

1.2 תביעה/ות 3-12,14-28 אינן מגדירות אמצאה שיש בה התקדמות המצאתית כהגדרתה ב**סעיף 5 לחוק**, לאור האמור בפרסום D1 בשילוב ידע כללי של בעל המקצוע בתחום.

Regarding claims 3-12, 14-28, Skilled person would consider as obvious possibility to improve the data security by monitoring the packets traffic for detecting an abnormal traffic pattern, as suggested by those claims. Said traffic monitoring would not involve any surprising effect in respect to the problem of privacy protection, nor would it supplement special contribution in respect to the solution which recited by independent claim 1 and disclosed in D1, namely, inspecting packets content according to the user **privacy** preferences. It is pointed out that the examples which given in the supporting disclosure in relation to the 'pattern' monitoring are concerning with cyber threats, such as denial of service attacks, and not actually with the specific problem of protecting the user privacy. Thereby, it could be argue that employing the user privacy preferences in respect to the monitoring of the traffic pattern would not have any special advantage.

לפיכך תביעה/ות 3-12,14-28 נעדרות התקדמות המצאתית.

2. <u>התביעות</u>

2.1 תביעות מס' 1 אינן עומדות בהוראות **סעיף 13(א) לחוק** היות שהן אינן נובעות באופן סביר מהמתואר בפירוט:

Claim 1 is not properly supported by the specifications, contrary to article 5. Said claim recites that the communication data type is determined by a remote server, where as the disclosure describes that said determination is performed by the user device.

לפיכך, אין בפירוט הבקשה סימוכין למלוא היקף התביעות הנ"ל. עליכם לנמק מהו הסימוכין בפירוט הבקשה לתביעות הנ"ל כפי שהוגדרו, או לתקן את הגדרת ההיקף הנתבע בהתאם לסימוכין בפירוט.

<u>חובת המבקש לעדכן את הרשות</u>

תשומת לבכם ל**סעיף 18א לחוק** לעניין חובת המבקשת לעדכן את הרשות על כל שינוי שחל ברשימת האסמכתאות או הפרסומים כאמור ב**סעיף 18(א) לחוק** ו**סעיף 18ג לחוק** בדבר אמצעי האכיפה.

<u>הגשת תיקונים לפירוט במהלך בחינת הבקשה</u>

באם יבוצעו תיקונים בבקשת הפטנט, תשומת לבכם מופנית **לתקנה 22(א)**. יש לשלוח לרשות עותק מלא של חלק הבקשה שבו הוכנסו התיקונים תוך סימונם באופן ברור. יש לסמן תוספות בקו תחתי (כך: <u>דוגמא</u>) והשמטות בקו חוצה (כך: ~~דוגמא~~). **אין להגיש מחדש קבצים שלא תוקנו**.

לתשומת לבכם:

א) בהתאם לתקנות 22(ב) ו-42 במידה שהנכם מתקנים את הפירוט כדי להתגבר על הליקויים בהודעה זו, עליכם לפרט את הליקויים שהתיקונים באים לסלקם, ולנמק כיצד תיקון הפירוט מתקן את הליקוי.

ב) בהתאם להוראות חוזר רשם 034/2017-פטנטים, במידה שבחינת הבקשה החלה לאחר 27.03.2017, תיקון פירוט בדרך של החלפת האמצאה שנבחנה ואשר לגביה הועלה ליקוי, באמצאה אחרת, בין אם היא הופיעה בתביעות מלכתחילה ובין אם תוארה בלבד, גם אם היא נובעת מהתיאור, אינו מהווה תיקון הליקוי ויביא לשליחת הודעה לפני סירוב.

<u>השגה בפני הרשם</u>

על פי **סעיף 161 לחוק**, הנכם רשאים להשיג על החלטתי בפני רשם הפטנטים תוך ארבעה חודשים ממועד משלוח ההודעה.

ניתן לעיין בפרטי תיק הבקשה באתר הרשות בקישור:

http://www.ilpatsearch.justice.gov.il/UI/RequestDetails.aspx?ReqId=251683

בכבוד רב

נעם מרקוביץ
בוחן פטנטים בכיר
טלפון: 02-5651735
דואר אלקטרוני: noamm@justice.gov.il
ראש צוות: רונן להב

PEARL COHEN
Advocates, Patent Attorneys & Notaries

Pearl Cohen Zedek Latzer Baratz
Idan Frydman, Adv., Partner | IFrydman@PearlCohen.com | +972-3-303-9066

29 בנובמבר 2018

לכבוד
רשות הפטנטים
רח' אגודת ספורט הפועל 1
הגן הטכנולוגי, בניין 5
ירושלים 96951

לידי בוחן פטנטים בכיר, נועם מרקוביץ:

הנדון: **תשובה להודעה (פ.ק. 26) מיום 31.7.2018**
מספרכם: 251683
מספרנו: P-566702-IL

א .נ.,

בתשובה להודעת הלשכה שבנדון, הרינו מגישים בזאת:

- ☐ תזכיר / MEMORANDUM IN RESPONSE TO AN OFFICIAL ACTION
- ☐ תביעות בפורמט PDF בגרסה נקייה.
- ☐ עותק מסומן של עמודי תביעות 30-25 עם הדגשת מקום התיקונים על גבי נייר.
- ☐ עדכון עפ"י סעיף 18 לחוק הפטנטים:
המבקשת מודיעה בזאת שבשלב זה אינה מודעת לציטוטים נוספים אותם ניתן לדווח עפ"י סעיף 18 לחוק הפטנטים.

בברכה,

עידן פרידמן, עו"ד
פרל כהן צדק לצר ברץ

MEMORANDUM IN RESPONSE TO AN OFFICE ACTION DATED JULY 31, 2018 FOR ISRAELI PATENT APPLICATION 251683

Our Ref.: P-566702-IL

This Memorandum is being filed in response to the Office Action issued on July 31, 2018. A response to the Office Action dated July 31, 2018 is due November 30, 2018. Accordingly, this response is timely filed.

In response to the above mentioned Office Action, Applicant respectfully submits the following:

Amendments

Applicant hereby submits the following amendments:

Claims 1-28 on pages 25-30. New pages 25-30 replace pages 25-30 currently in the file.

Claims 1, 4, 5, 12, 14-16 and 24 have been amended.

Arguments

In the Office Action the Examiner rejected the pending claims 1, 2 and 13 under Section 4 of the Israel Patent Law for lack of novelty over D1: US2013/0318347. Applicant notes that in a phone call with the Examiner, it was noted by the Examiner that the correct reference should be US2013/0318347 (D1) and not the reference WO2013/103782 that was wrongly indicated in the Office Action, while a corrected Office Action with the proper reference number was not issued.

Applicant respectfully traverses this rejection at least in view of the remarks that follow.

D1 describes an architecture for a data sharing system (DSS) to ensure the privacy and security of users' personal information. The user's personally identifiable information is stored and transmitted in an encrypted form, and the key remains in the sole possession of the user and the user's friends/contacts within the system. According to paragraph [0221] of D1, the DSS determines the relevance of data packets of user data with respect to the type of media,

e.g. the media-specific "page" or "section" of the "user interface" being viewed by a user on his local computing device, and also its date of creation and/or uploading. The relevance of a packet of user data might also be affected by whether or not it is related to some other piece of user data, such as a comment on a photo, i.e. metadata related to the content of the data packet.

Applicant asserts that while D1 describes a data sharing system for privacy of users' personal information, D1 fails to teach determination of at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet during communication session as recited at least in amended independent claim 1.

To find the claimed element "determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request; and modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference", the Examiner, on page 2 of the Office Action, cites to paragraphs [0221], [0494] and [0804] of D1. Applicant asserts that D1 describes the DSS considering media type, such as text, image, video, to determine relevance of data packets of user data. Thus, D1 directly analyses and inspect the content of data packets of the user's data to determine relevance to the user's privacy preference, for example a comment on a photo as indicated in paragraph [0221].

In contrast, in the present application the determination of the at least one communication data type is carried out in accordance with characteristics of the communication data packet during communication session between the user's device and the remote server, such that the communication is not interrupted. As described in the present application, the management of private data includes data type mapping of characteristics of the communication data packet where a data type corresponds to a vector of characteristics of the data packet (for example an unknown type that corresponds to a particular vector with a set of characteristics), such that the content of the data packet is not read, analyzed and inspected thereby maintaining privacy. Thus, this vector of characteristics cannot be identified with the media type of D1 that is determined in accordance with the content of the user's data.

Furthermore, Applicant notes that while D1 mentions metadata in paragraphs [0500]-[0501], this refers to user defined privacy preferences and not metadata as the characteristics and/or behavior of the data packet of the present application. Specifically, D1 indicates:

"Metadata may include such things as: which mode of a multi-modal user interface (UI) was last selected by the user; the maximum age of the user data which the user wishes to see included in the collections of data presented to the user by the DSS client's UI; which elements of user data the user has specified to be hidden; for which presentation template(s) (or "skin(s)") has the user expressed a preference; etc".

Accordingly, D1 fails to teach determination of at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet during communication session as recited at least in amended independent claim 1. Similar arguments apply to amended independent claim 12, mutatis mutandis, where the communication data pattern is determined in accordance with a vector of behavior ranges for the dynamic data flow of the communication data packet during communication sessions.

Each of claims 2 and 13 depends, directly or indirectly, from one of independent claims 1 and 12, and therefore includes all the limitations of the independent claim from which it depends. Therefore, Applicant respectfully asserts that claims 2 and 13 are likewise allowable.

Therefore, applicant respectfully requests that this rejection be withdrawn.

In the Office Action the Examiner rejected claims 3-12 and 14-28 under Section 5 of the Israel Patent Law for lack of inventiveness over US2013/0318347 (D1) in view of general knowledge of a person skilled in the art.

Applicant respectfully traverses this rejection at least in view of the remarks that follow.

D1 has been discussed above, and that discussion is applicable here as well. Similar arguments apply to amended independent claims 12 and 24, mutatis mutandis, where the communication data type and/or communication data pattern during communication sessions are determined in accordance with characteristics and/or behavior range of the communication data packet.

Applicant notes that while D1 describes sharing data according to user defined preferences, the methods and systems recited in the claims cannot be obvious in view of D1 in combination with general knowledge since D1 fails to teach at least determination of data type based on characteristics of the communication data packets such that there is no need to read, analyze and inspect the content of the data packet and interfere in the communication as well as

undermine the privacy of that content. Since the data type are determined without content-based communication "hand-shake", the allowed data may be shared efficiently in accordance with the privacy policy of the user.

Moreover, Applicant notes that the communication data pattern determined based on the behavior range of the communication data packet may be an alternative to the determined data type for dynamic management of private data according to the user's privacy preferences, for instance as described in paragraph [073] of the present application. Such determination of the communication data pattern cannot be achieved by D1 and is not obvious in view of D1 in combination with general knowledge.

Each of claims 3-11, 14-23 and 25-28 depends, directly or indirectly, from one of independent claims 1, 12 and 24, and therefore includes all the limitations of the independent claim from which it depends. Therefore, Applicant respectfully asserts that claims 3-11, 14-23 and 25-28 are likewise allowable.

Therefore, applicant respectfully requests that this rejection be withdrawn.

In the Office Action the Examiner objected to claim 1 under Section 13 of the Israel Patent Law for lack of support in the description of the present application.

Applicant respectfully traverses this rejection at least in view of the remarks that follow.

Applicant asserts that support for the communication data type determination being carried out by the remote server can be found at least in paragraphs [058]-[067] in regard to Figure 4 where the determination is carried out by the processor "402" which is not the user's device.

Therefore, applicant respectfully requests that this rejection be withdrawn.

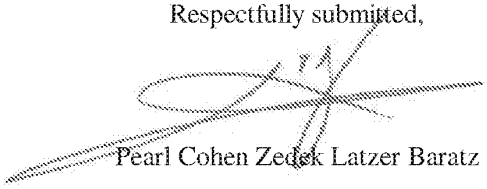
Duty to disclose

With respect to the duty to disclose new citations under Section 18, Applicant submits that there are no new citations to report.

In view of the foregoing amendments, the present response is believed to place the application

in condition for allowance. Favorable consideration and allowance of the application is therefore requested.

Respectfully submitted,



Pearl Cohen Zedek Latzer Baratz

P-566702-IL

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA
First Named Inventor/Applicant Name:	Yoseph KOREN
Filer:	Devorah N Livneh/Sigal Vegh
Attorney Docket Number:	P-566702-US

Filed as Small Entity

Filing Fees for U.S. National Stage under 35 USC 371

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
BASIC NATIONAL STAGE FEE	2631	1	150	150
NATL STAGE SEARCH FEE - REPORT PROVIDED	2642	1	260	260
NATL STAGE EXAM FEE - ALL OTHER CASES	2633	1	380	380
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**790**

Electronic Acknowledgement Receipt	
EFS ID:	37376656
Application Number:	16603252
International Application Number:	PCT/IL2018/050359
Confirmation Number:	6147
Title of Invention:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA
First Named Inventor/Applicant Name:	Yoseph KOREN
Customer Number:	49443
Filer:	Devorah N Livneh/Sigal Vegh
Filer Authorized By:	Devorah N Livneh
Attorney Docket Number:	P-566702-US
Receipt Date:	07-OCT-2019
Filing Date:	
Time Stamp:	05:58:08
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$790
RAM confirmation Number	E201907659103579
Deposit Account	602041
Authorized User	Sigal Vegh
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 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)

37 CFR 1.492 (National application filing, search, and examination fees)

37 CFR 1.492(a) (Basic national fee only)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		P-566702-US-U-APP-07OCT19.pdf	20738441 cc44505c32d5354ddf8906f6ce0035e4f1eb1632	yes	77

Multipart Description/PDF files in .zip description

Document Description	Start	End
Transmittal of New Application	1	3
Documents submitted with 371 Applications	4	47
Oath or Declaration filed	48	49
Transmittal Letter	50	52
Information Disclosure Statement (IDS) Form (SB08)	53	54
Other Reference-Patent/App/Search documents	55	55
Preliminary Amendment	56	56
Specification	57	57
Claims	58	63
Applicant Arguments/Remarks Made in an Amendment	64	64
Application Data Sheet	65	70
Internet Communications Authorized	71	71
Power of Attorney	72	72
Assignee showing of ownership per 37 CFR 3.73	73	77

Warnings:

Information:

2	Petition to make special under Patent Prosecution Hwy	P-566702-US-U-PPH-07OCT19-1.pdf	981885 09bcca055617185b8670b628a47e8cfb8f2ccf8e	no	21
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	35230 eae8f884c16c6cbfce1796f7fe4147e97c31da0f	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	21755556	

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.

<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.
<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.
<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.

Doc Code: ECOMM.AUTH/ECOMM.WTDW
Doc Description: Internet Communications Authorized/Internet Communications Authorization Withdrawn

PTO/SB/439 (11-15)

AUTHORIZATION FOR INTERNET COMMUNICATIONS IN A PATENT APPLICATION OR REQUEST TO WITHDRAW AUTHORIZATION FOR INTERNET COMMUNICATIONS		
	Application No.	**Not yet assigned**
	Filing Date	**Herewith**
	First Named Inventor	**Yoseph KOREN**
	Art Unit	**Not yet assigned**
	Examiner Name	**Not yet assigned**
	Practitioner Docket No.	**P-566702-US**

To: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I. To authorize permission for Internet Communications.

☒ Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with the undersigned and practitioners in accordance with 37 CFR 1.33 and 37 CFR 1.34 concerning any subject matter of this application via video conferencing, instant messaging, or electronic mail. I understand that a copy of these communications will be made of record in the application file. (MPEP 502.03)

II. To withdraw authorization for Internet Communications.

☐ The authorization given on _____, to the USPTO to communicate with the undersigned and any practitioner in accordance with 37 CFR 1.33 and37 CFR 1.34 concerning any subject matter of this application via Internet communications such as video conferencing, instant messaging, or electronic mail is hereby withdrawn. I understand that the withdrawal is effective when approved rather than when received.

I am the

☐ applicant.

☒ attorney or agent of record. Registration number 71,347

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____

/Devorah N. Livneh, Reg. No. 71,347/
Signature

7 October 2019
Date

Devorah N. Livneh Reg. No. 71,347
Typed or printed name

(646) 878-0800
Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Juristic entities must be represented by a patent practitioner (see 37 CFR 1.31, which is applicable to any paper filed on or after September 16, 2012, that is presented on behalf of a juristic entity, regardless of application filing date). Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

PTO/AIA/80 (07-12)
Approved for use through 11/30/2014. OMB 0651-0035
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 displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:

☒ Practitioners associated with the Customer Number: 49443

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name Registration	Number		Name Registration	Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:

☒ The address associated with Customer Number: 49443

OR

☐ Firm or Individual Name	[ ], Pearl Cohen Zedek Latzer Baratz LLP				
Address	1500 Broadway, 12th Floor				
City	New York	State	NY	ZIP	10036
Country	USA				
Telephone	(646) 878-0800	Email	USPTO@PearlCohen.com		

Assignee Name and Address:

Privacy Rating Ltd.
91/33 Hagalil St.
Ganey-Tikva 5891491
Israel

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of the practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Privacy Rating LTD

Signature	315246287 - .D.N	Date	December 4 2018
Name	YOSEPH KOREN	Telephone	+1-(201)(2108899)
Title	Co-founder & C.E.O		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. 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 3 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.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. 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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: **Yoseph KOREN et al.** Docket No.: **P-566702-US**

Application No./Patent No.: **Not yet assigned** Filed/Issue Date: **Herewith**

Titled: **SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA**

Privacy Rating Ltd. , a **Corporation** ,

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

   ☐ The extent (by percentage) of its ownership interest is _____ %. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

   ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

   Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

   The document was recorded in the United States Patent and Trademark Office at

   Reel _____, Frame _____, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). 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. 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.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. 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 displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Devorah N. Livneh, Reg. No. 71,347/	**7 October 2019**
Signature	Date
Devorah N. Livneh	**71,347**
Printed or Typed Name	Title or Registration Number

Docket No.: P-566702-US

ASSIGNMENT

In consideration of One Dollar ($1.00), and other good and valuable consideration, the Receipt of which is hereby acknowledged, we the undersigned, Yoseph KOREN residing at 91/33 Hagalil St., Ganey Tikva 5591491, Israel and Yehonatan WASSERMAN residing at 39 Kaplan St., Kiryat Ono 5529339, Israel (hereinafter, the "Assignor")

Hereby sell, assign and transfer to Privacy Rating Ltd., an Israeli company located at 91/33 Hagalil St., Ganey Tikva 5591491, Israel; its successors, assigns and legal representatives (hereinafter, the "Assignee"), the entire right, title and interest for all countries, in and to any and all inventions which are disclosed and claimed, and as possessed by the undersigned, any and all inventions which are disclosed but not claimed in the application for United States Application No. (_____, filed _____), which is a National Phase Application of PCT International Application No. PCT/IL2018/050359, PCT International filing date March 28, 2018 and being entitled:

SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

and in and to said application and all divisional, continuing, substitute, renewal, reissue, and all other applications for U.S. Letters Patent or other related property rights in any and all foreign countries which have been or shall be filed on any of said inventions disclosed in said application, including but not limited to prior Israeli Application 251683 filed on April 9, 2017; and in and to all original and reissued patents or related foreign documents which have been or shall be issued on said inventions; and including the Assignor's right in and to all revenue, income, royalties, damages and payments now or hereafter due or payable with respect to any Letters Patent which may be granted, and in and to all causes of action (either in law or in equity), and the right to sue, counterclaim, and recover for past, present and future infringement of the rights assigned or to be assigned under this Assignment. I hereby authorize and request the attorney of record of the firm Pearl Cohen Zedek Latzer Baratz LLP, 1500 Broadway, 12th Floor, New York 10036, to insert in the parentheses above, the filing date and US Serial No. of said application when known;

Authorize and request the Commissioner of Patents of the United States to issue to said Assignee, the corporation above named, its successors, assigns and legal representatives, in accordance with this assignment, any and all United States Letters Patent on said inventions or any of them disclosed in said application;

Agree that said Assignee may apply for and receive foreign Letters Patent or rights of any other kind for said inventions, or any of them; and may claim, in applications for said foreign Letters Patent or other rights, the priority of the aforesaid United States patent application under the provisions of the

International Convention of 1883 and later modifications thereof, under the Patent Cooperation Treaty, under the European Patent Convention or under any other available international agreement; and that, when requested, without charge to, but at the expense of, said Assignee, its successors, assigns and legal representatives, to carry out in good faith the intent and purpose of this assignment, the under-signed or the undersigned's executors or administrators will, for the United States and all foreign countries, execute all divisional, continuing, substitute, renewal, reissue, and all other patent applications or other documents on any and all said inventions; execute all rightful oaths, assignments, powers of attorney and other papers; communicate to said Assignee, its successors, assigns and representatives, all facts known and documents available to the undersigned relating to said inventions and the history thereof; testify in all legal proceedings; and generally do everything possible which said Assignee, its successors, assigns or representatives shall consider desirable for aiding in securing, maintaining and enforcing proper patent protection for said inventions and for vesting title to said inventions and all applications for patents or related foreign rights and all patents on said inventions, in said Assignee, its successors, assigns and legal representatives; and

COVENANT with said Assignee, its successors, assigns and legal representatives that no assignment, grant, mortgage, license or other agreement affecting the rights and property herein conveyed has been made to others by the undersigned, and that full right to convey the same as herein expressed is possessed by the undersigned.

FULL NAME OF INVENTOR: **Yoseph KOREN**	FULL NAME OF WITNESS:
SIGNATURE OF INVENTOR:	SIGNATURE OF WITNESS:
DATE: 03 /16 /2019 (day / month / year)	ADDRESS OF WITNESS:

Docket No.: P-566702-US

FULL NAME OF INVENTOR: **Yehonatan WASSERMAN**	FULL NAME OF WITNESS:
SIGNATURE OF INVENTOR:	SIGNATURE OF WITNESS:
DATE: 03/10/2019 (day / month / year)	ADDRESS OF WITNESS:

PTO/SB/08a (07-09)
Approved for use through 07/31/2012. 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.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	1	of	2

Complete if Known	
Application Number	Not yet assigned
Filing Date	Herewith
First Named Inventor	Yoseph KOREN
Art Unit	Not yet assigned
Examiner Name	Not yet assigned
Attorney Docket Number	P-566702-US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A	US-2013/318347	11-28-2013	MOFFAT BRIAN LEE	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
						☐
						☐
						☐
						☐
						☐
						☐
						☐
						☐

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

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 2 hours 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, 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 (1-800-786-9199) and select option 2.

PTO/SB/08b (07-09)
Approved for use through 07/31/2012. 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.

Substitute for form 1449B/PTO **INFORMATION DISCLOSURE STATEMENT BY APPLICANT** *(use as many sheets as necessary)*				***Complete if Known***	
				Application Number	**Not yet assigned**
				Filing Date	**Herewith**
				First Named Inventor	**Yoseph KOREN**
				Art Unit	**Not yet assigned**
(use as many sheets as necessary)				Examiner Name	**Not yet assigned**
Sheet	**2**	of	**2**	Attorney Docket Number	**P-566702-US**

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (where appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	B	Internatioanl Search Report of PCT Application No. PCT/IL2018/050359 mailed on July 12, 2018	☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐

Examiner Signature		Date Considered	

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

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 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 2 hours 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, 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 (1-800-786-9199) and select option 2.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2018/050359

A. CLASSIFICATION OF SUBJECT MATTER
IPC (2018.01) H04L 29/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC (2018.01) H04L 29/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Databases consulted: Esp@cenet, Google Patents
Search terms used: privacy communication data type and communication data pattern of "data packet";

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013318347 A1 MOFFAT BRIAN LEE?[US] 28 Nov 2013 (2013/11/28) ¶ 78, 149, 221, 232, 494, 499-501, 804	1-28

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"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)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 Jul 2018	12 Jul 2018
Name and mailing address of the ISA: Israel Patent Office Technology Park, Bldg 5, Malcha, Jerusalem, 9695101, Israel Facsimile No. 972-2-5651616	Authorized officer MARCOWITZ Noam Telephone No. 972-2-5651735

Form PCT/ISA/210 (second sheet) (January 2015)

Attorney Docket No.: P-566702-US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Yoseph KOREN et al.	Examiner:	Not yet assigned
Serial No.:	Not yet assigned	Group Art Unit:	Not yet assigned
Filed:	Herewith	Confirmation No.:	Not yet assigned
Title:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA		

PRELIMINARY AMENDMENT

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

Sir/Madam:

Prior to Examination, kindly amend the above-identified application as follows:

Amendments to the Specification begin on page **2** of this Amendment.

Amendments to the Claims are reflected in the listing of claims which begins on page **3** of this paper.

Remarks/Arguments begin on page **9** of this paper.

AMENDMENTS TO SPECIFICATION

In the Specification:

On page 1, after the title, please insert the following:

-- CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a National Phase Application of PCT International Application No. PCT/IL2018/050359, International Filing Date March 28, 2018, claiming the benefit of Israel Patent Application No. 251683, filed April 9, 2017, each of which is hereby incorporated by reference.--

AMENDMENTS TO THE CLAIMS

Please amend claims 1, 4, 12, 15 and 24.

Please cancel claims 6, 10, 11, 16, 21-23 and 25 without prejudice.

This listing of claims will replace all prior versions, and listings, of claims in this application:

Listing of Claims:

1. **(Currently Amended)** A method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request;

determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet;

receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication;

modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference; and

maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

2. (Original) The method of claim 1, wherein the communication data type of the at least one data packet is determined from metadata of communication with the remote server.

3. (Original) The method of claim 1, further comprising:

determining, by the user's device, at least one communication data pattern of at least one data packet corresponding to the received request; and

modifying data packets corresponding to requests for sharing of responses corresponding to at least one data pattern, that are not compatible with the received privacy preference,

wherein the privacy preference comprises a list of allowed data patterns for sharing during communication.

4. **(Currently Amended)** The method of claim [[1]]3, wherein the communication data pattern is determined based on a range selected from a group consisting of: data packet frequency, data packet size, data packet speed, data packet count, data packet ratio compared to other data type flow, data packet repentance, and data packet order.

5. (Original) The method of claim 1, wherein the communication data type is determined based on data packet characteristics selected from a group consisting of: data packet header, data packet footer, version number, IP address, HTTPS, file extension, encryption method, encoding method, keywords, driver, and communication protocol.

6. **(Canceled)**

7. (Original) The method of claim 1, further comprising:

determining, by the remote server, the communication data pattern of the at least one data packet of the received request; and

linking at least one response from the user's device to a type of data packet from the user's device, wherein the linking is based on the communication data type and communication data pattern of the at least one response.

8. (Original) The method of claim 1, further comprising:

identifying a response corresponding to a request for sharing of data packets, wherein the identified response is not compatible with the received privacy preference; and

providing a response with at least one modified data packet corresponding to the request for sharing types of data packets.

9. (Original) The method of claim 8, wherein the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

10. **(Canceled)**

11. **(Canceled)**

12. **(Currently Amended)** A method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request;

determining, by the remote server, at least one communication data pattern corresponding to the received request, wherein the at least one communication data pattern is determined in accordance with a behavior range of the communication data packet;

receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data patterns for sharing during communication;

modifying data packets corresponding to requests for sharing of responses and corresponding data patterns that are not compatible with the received privacy preference; and

maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

13. (Original) The method of claim 12, wherein the communication data pattern of the at least one response is determined from metadata of communication with the remote server.

14. (Original) The method of claim 12, further comprising:

determining, by the remote server, the communication data type of the at least one data packet of the received request; and

modifying data packets corresponding to requests for sharing of responses and corresponding data patterns, corresponding to at least one communication data packet type, that are not compatible with the received privacy preference,

wherein the privacy preference comprises a list of allowed data packet types for sharing during communication.

15. **(Currently Amended)** The method of claim [[12]]14, wherein the communication data type is determined based on data packet characteristics selected from a group consisting of: data packet header, data packet footer, version number, IP address, HTTPS, file extension, encryption method, encoding method, keywords, driver, and communication protocol.

16. **(Canceled)**

17. (Original) The method of claim 12, wherein the user's device is in communication with an external database with at least one communication data pattern corresponding to a request for sharing of data packets from the user's device, and wherein the at least one data pattern compatible with the received request is determined from the database.

18. (Original) The method of claim 12, further comprising:

determining, by the remote server, the type of the at least one data packet of the received request; and

linking at least one data pattern to a type of data packet from the user's device, wherein the linking is based on the communication data type and the communication data pattern of the at least one response.

19. (Original) The method of claim 12, further comprising:

identifying a communication data pattern corresponding to a request for sharing of data packet types, wherein the identified data pattern is not compatible with the received privacy preference; and

providing a response with at least one modified data packet corresponding to the request for sharing types of data packets.

20. (Original) The method of claim 19, wherein the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

21. **(Canceled)**

22. **(Canceled)**

23. **(Canceled)**

24. **(Currently Amended)** A system for dynamic management of private data during communication between a remote server and at least one user's device, the system comprising:

a communication data type database, comprising at least one communication data type corresponding to sharing of at least one data packet from the user's device;

a privacy preference database, comprising a list of allowed types of data packets for sharing during communication with the at least one user's device;

a communication module, to allow communication between the remote server and the at least one user's device; and

a processor, coupled to the response database and to the privacy preference database, wherein the processor is configured to instruct the remote server to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of

data packets for sharing, and wherein the at least one data type is determined in accordance with characteristics of the communication data packet.

25. **(Canceled)**

26. (Original) The system of claim 24, further comprising a communication data pattern database, coupled to the processor and comprising at least one data pattern corresponding to sharing of at least one data packet from the user's device, wherein the processor is configured to modify data packets corresponding to requests for retrieval of data packets and communication data types that are not compatible with communication data patterns from a communication data pattern database.

27. (Original) The system of claim 26, wherein data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

28. (Original) The system of claim 26, wherein at least the communication module and the processor are embedded on a single hardware component.

REMARKS

Applicants request entry of the Preliminary Amendment.

Applicants have amended claims 1, 4, 12, 15 and 24.

Applicants have canceled claims 6, 10, 11, 16, 21-23 and 25 without prejudice or disclaimer.

The subject Application is a National Phase Application of PCT International Application No. PCT/IL2018/050359, International Filing Date March 28, 2018, claiming the benefit of Israel Patent Application No. 251683, filed April 9, 2017.

Should the Examiner have any question or comment as to the form, content or entry of this Amendment, the Examiner is requested to contact the undersigned at the telephone number below.

To the extent any fees are due, those fees are being paid by credit card and/or deposit account. However, to the extent that the fees due are not specifically paid, please charge any fees associated with this paper to deposit account No. 60-2041.

Respectfully submitted,

/Devorah Livneh, Reg. No. 71,347/

Devorah N. Livneh
Attorney/Agent for Applicant(s)
Registration No. 71,347

Dated: October 7, 2019

Pearl Cohen Zedek Latzer Baratz LLP
1500 Broadway, 12th Floor
New York, New York 10036
Tel: (646) 878-0800
Fax: (646) 878-0801

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	P-566702-US
	Application Number	

Title of Invention	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

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
	Yoseph		KOREN	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Ganey Tikva	State/Province		Country of Residence	Israel

Mailing Address of Inventor:

Address 1	91 Hagalil St.
Address 2	

City	Ganey Tikva	State/Province	
Postal Code	5591491	Country	Israel

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Yehonatan		WASSERMAN	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Kiryat Ono	State/Province		Country of Residence	Israel

Mailing Address of Inventor:

Address 1	39 Kaplan St.
Address 2	

City	Kiryat Ono	State/Province	
Postal Code	5529339	Country	Israel

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	P-566702-US
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA	

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).		
☐ An Address is being provided for the correspondence Information of this application.		
Customer Number	49443	
Email Address	USPTO@PearlCohen.com	Add Email / Remove Email

Application Information:

Title of the Invention	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA		
Attorney Docket Number	P-566702-US	Small Entity Status Claimed ☒	
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	10	Suggest Figure for Publication (if any)	

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:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	49443		

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	P-566702-US
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA	

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this 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		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	a 371 of international	**PCT/IL2018/050359**	**2018-03-28**
Prior Application Status			Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)

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(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(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	Filing Date (YYYY-MM-DD)	Access Code (if applicable)
251683	**Israel**	**2017-04-09**	

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.

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.

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	P-566702-US
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA	

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.

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

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.

Clear

○ 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:

Name of the Deceased or Legally Incapacitated Inventor :	
If the Assignee is an Organization check here. ☒	

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	P-566702-US
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA	

Organization Name	Privacy Rating Ltd.

Prefix	Given Name	Middle Name	Family Name	Suffix

Mailing Address Information For Applicant:			
Address 1	91/33 Hagalil St.		
Address 2			
City	Ganey Tikva	State/Province	
Country	Israel	Postal Code	5591491
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. 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.

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.

Prefix	Given Name	Middle Name	Family Name	Suffix

If the Assignee or Non-Applicant Assignee is an Organization check here. ☒

Organization Name	Privacy Rating Ltd.

Mailing Address Information For Assignee including Non-Applicant Assignee:			
Address 1	91/33 Hagalil St.		
Address 2			
City	Ganey Tikva	State/Province	
Country	Israel	Postal Code	5591491
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (08-12)
Approved for use through 01/31/2014. OMB 0651-0032
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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	P-566702-US
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA	

Signature:

Remove

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, alljoint 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	/Devorah N. Livneh, Reg. No. 71,347/			Date (YYYY-MM-DD)	2019-10-07
First Name	Devorah	Last Name	Livneh	Registration Number	71,347

Additional Signature may be generated within this form by selecting the Add button. Add

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.**

PTO-1390 (01-17)
Approved for use through 8/31/2019. OMB 0651-0021
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 displays a valid OMB control number.

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A SUBMISSION UNDER 35 U.S.C. 371

Attorney Docket No.	
P-566702-US	
U.S. Application No. (if known, see 37 CFR 1.5)	

International Application No.	International Filing Date	Priority Date Claimed
PCT/IL2018/050359	28-Mar-2018	09-Apr-2017

Title of Invention: **SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA**

First Named Inventor: **Yoseph KOREN**

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information.

1. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). NOTE: The express request under 35 U.S.C. 371(f) will not be effective unless the requirements under 35 U.S.C. 371(c)(1), (2), and (4) for payment of the basic national fee, copy of the International Application and English translation thereof (if required), and the oath or declaration of the inventor(s) have been received.

2. ☒ A copy of the International Application (35 U.S.C. 371(c)(2)) is attached hereto (not required if the International Application was previously communicated by the International Bureau or was filed in the United States Receiving Office (RO/US)).

3. An English language translation of the International Application (35 U.S.C. 371(c)(2))

   a. ☐ is attached hereto.

   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).

4. An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4))

   a. ☒ is attached.

   b. ☐ was previously filed in the international phase under PCT Rule 4.17(iv).

Items 5 to 8 below concern amendments made in the international phase.

PCT Article 19 and 34 amendments

5. ☐ Amendments to the claims under PCT Article 19 are attached (not required if communicated by the International Bureau) (35 U.S.C. 371(c)(3)).

6. ☐ English translation of the PCT Article 19 amendment is attached (35 U.S.C. 371(c)(3)).

7. ☐ English translation of annexes (Article 19 and/or 34 amendments only) of the International Preliminary Examination Report is attached (35 U.S.C. 371(c)(5)).

Cancellation of amendments made in the international phase

8a. ☐ Do not enter the amendment made in the international phase under PCT Article 19.

8b. ☐ Do not enter the amendment made in the international phase under PCT Article 34.

NOTE: A proper amendment made in English under Article 19 or 34 will be entered in the U.S. national phase application absent a clear instruction from applicant not to enter the amendment(s).

The following items 9 to 17 concern a document(s) or information included.

9. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.

10. ☒ A preliminary amendment.

11. ☒ An Application Data Sheet under 37 CFR 1.76.

12. ☐ A substitute specification. NOTE: A substitute specification cannot include claims. See 37 CFR 1.125(b).

13. ☒ A power of attorney and/or change of address letter.

14. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13*ter*.3 and 37 CFR 1.821 - 1.825.

15. ☐ Assignment papers (cover sheet and document(s)). Name of Assignee:

16. ☒ 37 CFR 3.73(c) Statement (when there is an Assignee).

This collection of information is required by 37 CFR 1.414 and 1.491-1.492. 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 15 minutes to complete, including gathering information, preparing, and submitting the completed 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: Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

U.S. APPLN. No. (if known - see 37 CFR 1.5)	INTERNATIONAL APPLICATION No.	ATTORNEY DOCKET No.
	PCT/IL2018/050359	P-S66702-US

17. ☐ Other items or information:

The following fees have been submitted.	CALCULATIONS	PTO USE ONLY
18. ☒ Basic National Fee (37 CFR 1.492(a)) $300	$ 300	
19. ☒ Examination Fee (37 CFR 1.492(c)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) ..... $0 All other situations $760	$ 760	
20. ☒ Search Fee (37 CFR 1.492(b)) If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4) ..... $0 Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority ..... $140 International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB ..... $520 All other situations $660	$ 520	
TOTAL OF 18, 19, and 20 =	$ 1580	
☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing in compliance with 37 CFR 1.821(c) or (e) in an electronic medium or computer program listing in an electronic medium) (37 CFR 1.492(j)). Fee for each addition 50 sheets of paper or fraction thereof $400		

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof (round up to a whole number)	RATE	
- 100 =	/ 50 =		x $400	$
Surcharge of $140.00 for furnishing any of the search fee, examination fee, or the oath or declaration after the date of commencement of the national stage (37 CFR 1.492(h)).				$

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	- 20 =		x $100	$	
Independent claims	- 3 =		x $460	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ $820	$	
Processing fee of $140.00 for furnishing the English translation later than 30 months from the earliest claimed priority date (37 CFR 1.492(i)).			+	$	
TOTAL OF ABOVE CALCULATIONS =				$ 1580	
☒ **Applicant asserts small entity status.** See 37 CFR 1.27. Fees above are reduced by ½.					
☐ **Applicant certifies micro entity status.** See 37 CFR 1.29. Fees above are reduced by ¾. Applicant must attach form PTO/SB/15A or B or equivalent.					
TOTAL NATIONAL FEE =				$ 790	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property.			+	$	
TOTAL FEES ENCLOSED =				$ 790	
				Amount to be refunded:	$
				Amount to be charged:	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. **50-3355** in the amount of **$**_____ to cover the above fees.

c. ☒ To the extent that there are any fees associated with this filing that are due but are not paid or are not able to be paid by a credit card mentioned elsewhere in this document, Applicants authorize the U.S. Patent and Trademark Office to charge any such fees to Deposit Account No. **50-2041** as follows:

i. ☐ any required fee.

ii. ☒ any required fee except for excess claims fees required under 37 CFR 1.492(d) and (e) and multiple dependent claim fee required under 37 CFR 1.492(f).

d. ☐ Fees are to be charged to a credit card. **WARNING**: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. The PTO-2038 should only be mailed or faxed to the USPTO. However, when paying the basic national fee, the PTO-2038 may NOT be faxed to the USPTO.

ADVISORY: If filing by EFS-Web, do **NOT** attach the PTO-2038 form as a PDF along with your EFS-Web submission. Please be advised that this is not recommended and by doing so your **credit card information may be displayed via PAIR**. To protect your information, it is recommended to pay fees online by using the electronic payment method.

NOTE: Where an appropriate time limit under 37 CFR 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the international Application to pending status.

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 1: 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**.

NOTE 2: A U.S. national stage application may not claim priority to the international application of which it is the national phase. The filing date of a U.S. national stage application is the international filing date. See 35 U.S.C. 363.

Correspondence Address

☒ The address associated with Customer Number: **49443 OR** ☐ Correspondence address below

Name	**PEARL COHEN ZEDEK LATZER BARATZ LLP**				
Address	**1500 Broadway, 12th Floor**				
City	**New York**	State	**New York**	Zip Code	**10036**
Country	**USA**	Telephone	**(646) 878-0800**		
Email	**USPTO@PearlCohen.com**				

Signature	/Devorah N. Livneh, Reg. No. 71,347/	Date	**07 October 2019**
Name (Print/Type)	Devorah N. Livneh	Registration No. (Attorney/Agent)	**71,347**

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 October 2018 (18.10.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/189736 A1

(51) International Patent Classification:
H04L 29/12 (2006.01)

(21) International Application Number:
PCT/IL2018/050359

(22) International Filing Date:
28 March 2018 (28.03.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
251683 09 April 2017 (09.04.2017) IL

(72) Inventor; and
(71) Applicant: **KOREN, Yoseph** [IL/IL]; 91/33 Hagalil street, 5591491 Ganey-Tikva (IL).

(72) Inventor: **WASSERMAN, Yehonatan**; 39 Kaplan St., 5529339 Kiryat-Ono (IL).

(74) Agent: **FRYDMAN, Idan** et al.; Pearl Cohen Zedek Latzer Baratz, P.O. Box 7198, 6107121 Tel Aviv (IL).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, 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:
— *with international search report (Art. 21(3))*

(54) **Title:** SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

(57) **Abstract:** Systems and methods of dynamic management of private data during communication between a remote server and a user's device, including receipt of a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request, determination of at least one communication data type of the at least one data packet correspondin g to the received request, receipt of a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication, modification of data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference and maintenance of communication between the remote server and the user's device, with sharing of the modified data packet.

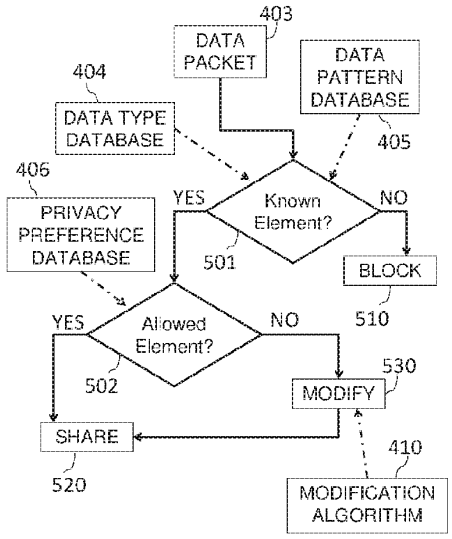


Fig. 5

WO 2018/189736 A1

SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

FIELD OF THE INVENTION

[001] The present invention relates to data management. More particularly, the present invention relates to systems and methods for dynamic management of private data.

BACKGROUND OF THE INVENTION

[002] During communication with external remote servers different types of data are automatically (and uncontrollably) shared, sometimes without the knowledge of the user (e.g., the owner of the data). There are currently only limited ways for the user to manage which data should be shared, with which parties, and at what time periods and/or under what circumstances such that privacy agreements cannot be fully enforced. For example, securing private elements of a user's device engaging in a transaction with a service provider, has been a challenge for many years with the rapid development of computer technology.

[003] In recent years, an increasing number of communication sessions are being biased (in terms of shared data and application usage) toward one party which is advantageous due to technological superiority, formal regulation power, and/or any other item. Such biasing may occur due to rapid development of communication related software, as well as due to development of computer technology.

[004] Social network service providers usually collect user (private) data, for example collect user's online habits. Data collection is usually carried out by a service provider requesting to share user's (private) information while the user's device automatically shares the requested information accordingly. Actions are executed by dedicated software (e.g., social plug in), which upload data requests when visiting web sites and/or applications. Such requests may be direct script by the service provider (e.g. cookie etc.), or indirect script hidden within links to other (partner) application provider (e.g. social plug-in, SDK, API etc.). While some devices allow blocking collection of certain private parameters, for example the location, only data emerging from sensors, such as global positioning system (GPS) sensors, can be managed by user while other sources of location (e.g. mobile network, IP provider, country, time zone) cannot be controlled so that in that case location information can still be collected. Thus, location information can be collected

while bypassing the instructions of the user (e.g., collecting location from cellular carrier data). Other examples from the same nature may include retrieving form data, retrieving data from flash memory and several other items which do not have the full (or partial) ability to disable and/or block data collection. Some service providers can also collect user data in order to transfer and/or sell to third parties (e.g., to present dedicated ads in the future). Another example may be avoiding biased exchange of information both from the user and the service provider perspectives.

SUMMARY OF THE INVENTION

[005] There is thus provided, in accordance with some embodiments of the invention, a method of dynamic management of private data during communication between a remote server and a user's device, the method including receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request, determining, by the user's device, the data type of the at least one data packet corresponding to the received request, receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference includes a list of allowed data packet types for sharing during communication, modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference, and maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

[006] In some embodiments, the type of the at least one data packet may be determined from metadata of communication with the remote server. In some embodiments, the method further includes determining, by the user's device, pattern of at least one response corresponding to the received request, and modifying data packets corresponding to requests for sharing of responses, corresponding to at least one data pattern, that are not compatible with the received privacy preference, wherein the privacy preference includes a list of allowed data patterns for sharing during communication. In some embodiments, the user's device includes a database with at least one data packet type corresponding to a request for sharing of data packets from the user's device, and wherein the type of data packets is determined from the database.

[007] In some embodiments, the method further includes linking at least one response to a type of data packet from the user's device, wherein the linking is based on the type and pattern of the at least one response. In some embodiments, the method further includes identifying a response corresponding to a request for sharing of data packets, wherein the identified response is not compatible with the received privacy preference, and providing a response with at least one modified data packet corresponding to the request for sharing types of data packets. In some embodiments, the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

[008] In some embodiments, the method further includes identifying a communication pattern between the server and the user's device, wherein the communication pattern includes at least one request for retrieval of at least one data packet from the user's device and corresponding responses, and issuing an alert upon detection of a change in the identified communication pattern.

[009] In some embodiments, data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

[010] There is thus provided, in accordance with some embodiments of the invention, a method of dynamic management of private data during communication between a remote server and a user's device, the method including receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request, determining, by the user's device, at least one data pattern corresponding to the received request, receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference includes a list of allowed data patterns for sharing during communication, modifying data packets corresponding to requests for sharing of responses and corresponding data patterns that are not compatible with the received privacy preference, and maintaining communication between the remote server and the user's device, with sharing of the modified responses.

[011] In some embodiments, the pattern of the at least one response is determined from metadata of communication with the remote server. In some embodiments, the method further includes determining, by the user's device, the type of the at least one data packet of the received request, and modifying data packets corresponding to requests for sharing of responses and corresponding data patterns, corresponding to at least one data packet type, that are not compatible with the received privacy preference, wherein the privacy preference includes a list of allowed data packet types for sharing during communication.

[012] In some embodiments, the user's device includes a database with at least one data pattern corresponding to a request for sharing of data packets from the user's device, and wherein the at least one data pattern compatible with the received request is determined from the database. In some embodiments, the method further includes determining, by the user's device, the type of the at least one data packet of the received request, and linking at least one data pattern to a type of data packet from the user's device, wherein the linking is based on the pattern of the at least one response.

[013] In some embodiments, the method further includes identifying a data pattern corresponding to a request for sharing of data packet types, wherein the identified data pattern is not compatible with the received privacy preference, and providing a response with at least one modified data packet corresponding to the request for sharing types of data packets. In some embodiments, the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

[014] In some embodiments, the method further includes issuing an alert upon detection of a request for sharing data packets, wherein the detected request does not correspond to at least one of data type and data pattern that is compatible with the received privacy preference. In some embodiments, the method further includes identifying a communication pattern between the server and the user's device, wherein the communication pattern includes at least one request for retrieval of at least one data packet from the user's device and corresponding responses, and issuing an alert upon detection of a change in the identified communication pattern.

[015] In some embodiments, data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect

attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

[016] There is thus provided, in accordance with some embodiments of the invention, a system for dynamic management of private data during communication between a remote server and at least one user's device, the system including a data type database, including at least one data type corresponding to sharing of at least one data packet from the user's device, a privacy preference database, including a list of allowed types of data packets for sharing during communication with the at least one user's device, a communication module, to allow communication between the remote server and the at least one user's device, and a processor, coupled to the response database and to the privacy preference database, wherein the processor is configured to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of data packets for sharing.

[017] In some embodiments, the system further includes a user interface to issue an alert upon detection of a request for retrieval of data packets that is not compatible with the privacy preference. In some embodiments, the system further includes a data pattern database, coupled to the processor, wherein the processor is configured to modify data packets corresponding to requests for retrieval of data packets and data types that are not compatible with data patterns from a data pattern database.

[018] In some embodiments, data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory. In some embodiments, at least the communication module and the processor are embedded on a single hardware component.

BRIEF DESCRIPTION OF THE DRAWINGS

[019] The subject matter regarded as the invention is particularly pointed out and distinctly claimed in the concluding portion of the specification. The invention, however, both as to organization and method of operation, together with objects, features, and advantages thereof, may best be understood by reference to the following detailed description when read with the accompanying drawings in which:

[020] Fig. 1 shows a schematic block diagram of an exemplary computing device, according to some embodiments of the invention;

[021] Fig. 2 schematically illustrates a data mapping system, according to some embodiments of the invention;

[022] Fig. 3A schematically illustrates examplary mapping of data type database, according to some embodiments of the invention;

[023] Fig. 3B schematically illustrates examplary mapping of data pattern database, according to some embodiments of the invention;

[024] Fig. 3C schematically illustrates examplary mapping of privacy preference table, according to some embodiments of the invention;

[025] Fig. 4 schematically illustrates a data management system, according to some embodiments of the invention;

[026] Fig. 5 shows a flowchart for a method of management of data packets with a sharing algorithm during communication between a remote server and a user's device, according to some embodiments of the invention;

[027] Figs. 6A-6B show flowcharts for a method of dynamic management of private data during communication between a remote server and a user's device, according to some embodiments of the invention; and

[028] Fig. 7 schematically illustrates a data management system 700 for dynamic management of private data that is embedded on a hardware component, according to some embodiments of the invention.

[029] It will be appreciated that for simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference numerals may be repeated among the figures to indicate corresponding or analogous elements.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[030] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will be understood by those skilled in the art that the present invention may be practiced without these specific

details. In other instances, well-known methods, procedures, and components have not been described in detail so as not to obscure the present invention.

[031] Although embodiments of the invention are not limited in this regard, discussions utilizing terms such as, for example, "processing," "computing," "calculating," "determining," "establishing", "analyzing", "checking", or the like, may refer to operation(s) and/or process(es) of a computer, a computing platform, a computing system, or other electronic computing device, that manipulates and/or transforms data represented as physical (e.g., electronic) quantities within the computer's registers and/or memories into other data similarly represented as physical quantities within the computer's registers and/or memories or other information non-transitory storage medium that may store instructions to perform operations and/or processes. Although embodiments of the invention are not limited in this regard, the terms "plurality" and "a plurality" as used herein may include, for example, "multiple" or "two or more". The terms "plurality" or "a plurality" may be used throughout the specification to describe two or more components, devices, elements, units, parameters, or the like. Unless explicitly stated, the method embodiments described herein are not constrained to a particular order or sequence. Additionally, some of the described method embodiments or elements thereof can occur or be performed simultaneously, at the same point in time, or concurrently.

[032] Reference is made to Fig. 1, showing a schematic block diagram of an exemplary computing device, according to embodiments of the present invention. Computing device 100 may include a controller 105 that may be, for example, a central processing unit processor (CPU), special purpose processor such as a graphic processing unit (GPU), communication control processing (CCP), a chip or any suitable computing or computational device, an operating system 115, a memory 120, a storage 130, an input devices 135 and an output device 140. Controller 105 may be configured to carry out methods as disclosed herein by for example executing code or software.

[033] Operating system 115 may be or may include any code segment designed and/or configured to perform tasks involving coordination, scheduling, arbitration, supervising, controlling or otherwise managing operation of computing device 100, for example, scheduling execution of programs. Operating system 115 may be a commercial operating system. Memory 120 may be or may include, for example, a Random Access Memory (RAM), a read only memory (ROM), a Dynamic RAM (DRAM), a Synchronous DRAM

(SD-RAM), a double data rate (DDR) memory chip, a Flash memory, a volatile memory, a non-volatile memory, a cache memory, a buffer, a short term memory unit, a long term memory unit, or other suitable memory units or storage units. Memory 120 may be or may include a plurality of, possibly different memory units.

[034] Executable code 125 may be any executable code, e.g., an application, a program, a process, automated task, software bots configured to manage data communication and user data collection (e.g., botnet), software adapted to perform artificial intelligence (AI), e.g. machine learning, deep learning, task or script. Executable code 125 may be executed by controller 105 possibly under control of operating system 115. Where applicable, executable code 125 may carry out operations described herein in real-time. Computing device 100 and executable code 125 may be configured to update, process and/or act upon information at the same rate the information, or a relevant event, are received. In some embodiments, more than one computing device 100 may be used. For example, a plurality of computing devices (in serial and/or parallel) that include components similar to those included in computing device 100 may be connected to a network and used as a system.

[035] Storage 130 may be or may include, for example, a hard disk drive, a universal serial bus (USB) device or other suitable removable and/or fixed storage unit. Content may be stored in storage 130 and may be loaded from storage 130 into memory 120 and may be stored in read only memory (ROM) to be loaded into memory 120 where it may be processed by controller 105. In some embodiments, some of the components shown in Fig. 1 may be omitted. For example, memory 120 may be a non-volatile memory having the storage capacity of storage 130. Accordingly, although shown as a separate component, storage 130 may be embedded or included in memory 120.

[036] Input devices 135 may be or may include a mouse, a keyboard, a touch screen or pad or any suitable input device. In some embodiments, computing device 100 receives input from a sensor such as global positioning system (GPS), camera, microphone, accelerometer, light sensor, compass, and any other sensor. It will be recognized that any suitable number of input devices may be operatively connected to computing device 100 as shown by block 135. Output devices 140 may include one or more displays, indicators, speakers, haptic output and/or any other suitable output devices. It will be recognized that any suitable number of output devices may be operatively connected to computing device 100 as shown by block 140. Any applicable input/output (I/O) devices may be connected

to computing device 100 as shown by blocks 135 and 140. For example, a wired or wireless network interface card (NIC), a modem, a universal serial bus (USB) device or external hard drive, cellular network connection, optical network connection, Bluetooth, and NFC may be included in input devices 135 and/or output devices 140.

[037] Embodiments of the invention may include an article such as a computer or processor non-transitory readable medium, or a computer or processor non-transitory storage medium, such as for example a memory, a disk drive, or a USB flash memory, encoding, including or storing instructions, e.g., computer-executable instructions, which, when executed by a processor or controller, carry out methods disclosed herein. For example, a storage medium such as memory 120, computer-executable instructions such as executable code 125 and a controller such as controller 105.

[038] Some embodiments may be provided in a computer program product that may include a non-transitory machine-readable medium, with instructions stored thereon, which may be used to program a computer, or other programmable devices, to perform methods as disclosed herein. Embodiments of the invention may include an article such as a computer or processor non-transitory readable medium, or a computer or processor non-transitory storage medium, such as for example a memory, a disk drive, or a USB flash memory, encoding, including or storing instructions, e.g., computer-executable instructions, which when executed by a processor or controller, carry out methods disclosed herein. The storage medium may include, but is not limited to, any type of disk including magneto-optical disks, semiconductor devices such as read-only memories (ROMs), random access memories (RAMs), such as a dynamic RAM (DRAM), erasable programmable read-only memories (EPROMs), flash memories, electrically erasable programmable read-only memories (EEPROMs), magnetic or optical cards, or any type of media suitable for storing electronic instructions, including programmable storage devices.

[039] A system according to embodiments of the invention may include components such as, but not limited to, a plurality of central processing units (CPU) or any other suitable multi-purpose or specific processors or controllers, a plurality of input units, a plurality of output units, a plurality of memory units, and a plurality of storage units. A system may additionally include other suitable hardware components and/or software components. In some embodiments, a system may include or may be, for example, a personal computer, a desktop computer, a mobile computer, a laptop computer, a notebook computer, a

terminal, a workstation, a server computer, a Personal Digital Assistant (PDA) device, a tablet computer, a network device, a smartphone, IOT device, action specific computerized machine (such as a dedicated robot) or any other suitable computing device. Unless explicitly stated, the method embodiments described herein are not constrained to a particular order or sequence. Additionally, some of the described method embodiments or elements thereof can occur or be performed at the same point in time.

[040] Reference is now made to Fig. 2, which schematically illustrates a data mapping system 200 for mapping of private data during communication with a remote server 201, according to some embodiments of the invention. The direction of arrows in Fig. 2 may indicate the direction of information flow. In order to manage private data for individual users, data mapping system 200 may initially map data types and data patterns (for example as a calibration process), as further described hereinafter. It should be noted that private data as used hereinafter may refer to any data and/or portion of data representing user's behavior, habits, characteristics, opinions, preferences, tendencies, relations, actions, status parameters (e.g., social, health, economic/wealth, legal, dependencies, being part of group and the like) and the like. In some embodiments, the user may be a computerized device (e.g., IOT, bot and the like) automatically operating on the user's behalf, so that the private data may refer to data and/or characteristics of the computerized device. Private data may also include privacy data and/or privacy preference(s).

[041] A user may choose based on private preference to share some private data and not to share other private data. Users may choose to share same private data with specific server and/or application and not to share it with different servers and/or application. In some embodiments, users may change such preference(s) at any applicable point in time. In some embodiments, private data may be automatically created to represent at least one feature of a computerized device and/or of the user of the computerized device. In some embodiments, private data may include at least one communication pattern and/or communication origin and destination and/or digital footprint and/or digital trace and/or digital response and/or digital reference. In some embodiments, private data may be received from analysis of data and/or from an external sensor and/or other source.

[042] The server 201 may be coupled to processor 202 such as controller 105, shown in Fig. 1. In some embodiments, processor 202 may receive at least one data packet 203 from server 201 to be mapped. For instance, processor 202 may receive at least one data packet

203 from a set of predetermined (or pre-classified) data packets 203. In some embodiments, processor 202 may receive from server 201 a request for sharing at least one data packet 203, for instance a request to share data packet with a contact name or contact directory data, where an automatic response may be created for each such request. It should be noted that data of such responses may also be considered as data packets 203 (e.g., to be mapped).

[043] In some embodiments, data mapping system 200 may include at least one data type database 204 and/or at least one data pattern database 205 and/or at least one privacy preference database 206 coupled to processor 202. In some embodiments, processor 202 may analyze the received data packet 203 to determine data type 207 of the data packet 203, for example by verifying at least one characteristic of the data packet 203. An examplary mapping of data types 207 is shown in Fig. 3A.

[044] In some embodiments, processor 202 may receive (e.g., from a user) privacy preference 209 to map the privacy preference database 206 for each data type and/or data pattern of the at least one data packet 203. In some embodiments, data mapping system 200 may include a modification algorithm 210, coupled to processor 202, and configured to, modify content of data packets according to at least one privacy preference 209 (e.g., nullify a content of a data packet). For example, the user may select a privacy preference 209 for forbidden sharing of location such that modification algorithm 210 may modify the content of the data packet 203 per a predetermined algorithm, for instance randomly modify the location (country) to any other country from a list of countries (e.g., Italy).

[045] Reference is now made to Fig. 3A, which schematically illustrates examplary mapping of data type database 204, according to some embodiments of the invention. Processor 202 may receive a request to share at least one data packet 203 (e.g., from server 201) and analyze characteristics of the at least one data packet 203, for example analyze characteristics of automatically created responses for the request. In some embodiments, the content of the received at least one data packet 203 may be analyzed for purposes of data type mapping.

[046] According to some embodiments, characteristics of the received at least one data packet 203 may be determined and dynamically fitted to an 'i'-dimensional vector 304 (e.g., static characteristics determined from metadata). It should be noted that while the characteristics vector 304 shown in Fig. 3A is five-dimensional, such vectors may have a

large number of characteristics. For example, an injective vector having dimensions of 50 characteristics (so that 'i'=50) or more. In some embodiments, an increased number of parameters in the characteristics vector 304 may improve chances of correctly determining the data type 207 until optimal determination of various data types may be achieved.

[047] At least one of the following characteristics of a data packet 203 may be injectively determined for each data packet: header, footer, version number, request by hostname/IP, sent to hostname/IP, server hostname/IP, IP address, file extension, , standard title, non-standard title, , encryption yes/no, encryption method, encoding yes/no, encoding method (e.g., 'UTF8'), whole file, chunked file, keywords, API version, SDK version, Social plug-in version, driver, communication protocol, action verbs, HTTP/HTTPS, URL Part Names, and/or any other specific character 'i' within the at least one data packet 203. The determined characteristics vector 304 may be associated with a particular data type 207 (since every data packet 203 corresponds to some data type 207), that may be still unknown (e.g., in terms of its content) and for instance indicated as data type 'j'. In some embodiments, processor 202 may receive at least one pre-classified data packet 203 with a known data type. In some embodiments, the data type 207 of characteristics vector 304 for the data-mapping stage, may be determined by reading the content of the corresponding data packet 203, for example reading content for the country name, web browsing history, operating system, etc.

[048] Such data types 207 (or characteristics vectors 304) that are gathered by processor 202, and possibly still having unknown data type content (e.g., data type 'j') at this stage, may be stored (e.g., stored in memory such as memory 120 shown in Fig. 1) at data type database 204 in order to carry out the data type mapping. Processor 202 may map the stored data types to link characteristics vectors 304 with data types 207. In some embodiments, processor 202 may determine that characteristics vectors 304 having at least one identical characteristic may correspond to a particular data type 207 (e.g. Web content search history type).

[049] Reference is now made back to Fig. 2. In some embodiments, data pattern database 205 may include at least one data pattern 208 corresponding to responses to sharing of at least one data packet 203. Similarly to mapping of data types (e.g., as shown in Fig. 3A), processor 202 may map data patterns of responses to request of sharing data packets 203. It should be noted that while the data type 207 of a data packet 203 may correspond to

static parameters (e.g., email address), the data patterns 208 may correspond to features of the dynamic data flow of data packet 203 that may be regarded as the "behavior" of the data packet 203.

[050] Reference is now made to Fig. 3B, which schematically illustrates examplary mapping of data pattern database 205, according to some embodiments of the invention. Processor 202 may receive at least one data packet 203 (e.g., from server 201), for example at least one response (or data packet) corresponding to a request for sharing the data packet 203 to analyze pattern behavior of the at least one response (or data packet). In some embodiments, the content of the received at least one data packet 203 may be analyzed to determine the data pattern. For example, at least one response may injectively correspond to a request for sharing at least one data packet 203 and/or a characteristic of the data packet 203 (e.g., a picture file from memory or from camera).

[051] It should be noted that while the pattern vector 305 shown in Fig. 3B is four-dimensional, such vectors may have a large number of features or ranges. For example, an injective vector 305 having dimensions of 100 features and/or ranges (so that 'm'=100) or more. At least one of the following dynamic features of a data pattern may be determined for each data packet: frequency (e.g., appearance(s) per second), size (e.g., in kilobytes), speed (in kilobytes per second), count (e.g., numbers), ratio (e.g., compared to other datatype flow), repeat (e.g., cyclic order), order, server reference (e.g., website reference such as "example.com/feature") and/or any combination thereof and/or other pattern behavior 'm' within the at least one data packet. In some embodiments, ranges for every feature (e.g., frequency) may be determined (e.g., lowest and highest frequency) as a feature of the data pattern 208. In some embodiments, a range may refer to non-discrete values (in contrast to discrete or static values in data type mapping, as shown in Fig. 3A), for instance a range defining number of website sub references (e.g., "example.com/sub-feature/sub-feature" with two sub references).

[052] The determined feature or pattern behavior vector 305 may be associated with a particular data pattern 208 (since every data packet 203 corresponds to some data pattern 208), that may be still unknown and for instance indicated as data pattern 208 'n'. In some embodiments, processor 202 may receive at least one pre-classified data packet 203 with a known data pattern.

[053] Such data patterns 208 that are gathered by processor 202, and possibly still having unknown data pattern 'n' at this stage, may be stored (e.g., stored in memory such as memory 120 shown in Fig. 1) at data pattern database 205 in order to carry out the data pattern mapping. Processor 202 may map the stored data patterns 'n' to link behavior vectors 305 with data patterns 208. In some embodiments, processor 202 may determine that pattern behavior vectors 305 having at least one identical characteristic and/or range may correspond to a data pattern 208 (e.g., same frequency range). In some embodiments, data patterns 208 may be determined according to logical conditions and/or ranges, for example for responses having frequency and size features in within predetermined thresholds.

[054] Reference is now made to Fig. 3C, which schematically illustrates examplary mapping of privacy preference table 306, according to some embodiments of the invention. Processor 202 may receive at least one data packet 203 (e.g., from server 201), for example at least one response (or data packet) corresponding to a request for sharing the data packet 203 to analyze type and pattern behavior of the at least one response (or data packet) to create data type database 204 and data pattern database 205 as described above. In some embodiments, processor 202 may receive (e.g., from a user) privacy preference database 206 to map the privacy preference table 306 for each data type (content) and/or data pattern of the at least one data packet 203. For example, the user may fill a privacy preference template (e.g., selecting to allow sharing of username) for different options of data types and/or data patterns to determine the privacy preference table 306. In case that some data packet is forbidden for sharing (e.g., contact data and/or a password), the content of that data packet may be, for example randomly, modified by predetermined modification algorithm 210 such that the modified content (e.g., nullified password or randomly replaced to a dummy contact name from a list) may be shared. In some embodiments, processor 202 may only check the data type such that no pattern is checked in order to determine the policy to apply, for example sharing of password data types may be completely forbidden so that data patterns are not checked. In some embodiments, processor 202 may detect an IoT device and only check the data pattern where the data type may not be checked. In some embodiments, processor 202 may only check the data pattern such that no data type is checked, for example checking frequency limit and modifying in accordance with the predefined limitations. In some embodiments,

repetition in at least one forbidden characteristic (e.g., forbidden frequency) may cause blocking of data sharing.

[055] Reference is now made back to Fig. 2. In some embodiments, privacy preference database 206 may include at least one privacy preference 209 such as a template to link privacy preferences for the determined data types 207 and/or data patterns 208 and/or modification algorithm 210. For example, privacy preference database 206 may include an un-populated matrix with data types 207 and/or data patterns 208 and/or modification algorithm 210 such that a user may choose which data types (content) 207 and/or data patterns 208 to share. In some embodiments, data mapping system 200 may include a modification algorithm 210, coupled to processor 202, and configured to manage sharing of at least one data packet 203 based on its data type 207 and/or data pattern 208 to comply with at least one privacy preference 209. The operation of the modification algorithm 210 is further described in Fig. 5, hereinafter.

[056] In some embodiments, data mapping system 200 (shown in Fig. 2) may be used as a system to determine collection of uncontrolled information from hardware equipment. Some manufacturers embed into their products, hidden agent(s) which transmits at least one hidden data packet. As may be apparent to one of ordinary skill in the art, such systems and methods may identify "back door" ability which may be part of the hardware core functionality and/or part of unit's embedded software. In some embodiments, by implementing the data mapping system 200 (shown in Fig. 2), unrecognized type and/or pattern of data packet may be determined, wherein the unrecognized type and/or pattern of data packet may be generated internally (in contrast to being requested by the server). Such data packet may be stored and further investigated for its origin and destination.

[057] Reference is now made to Fig. 4, which schematically illustrates a data management system 400 for dynamic management of private data during communication between a remote server 401 (such as server 201 in Fig. 2) and at least one user's device 411, according to some embodiments of the invention. The direction of arrows in Fig. 4 may indicate the direction of information flow. It should be noted that the at least one user's device 411 may be a computerized device such as computing device 100, shown in Fig. 1.

[058] In some embodiments, data management system 400 may include a data type database 404 (such as data type database 204 in Fig. 2), coupled to processor 402, such

that processor 402 may modify data packets (e.g., modify responses) to requests for retrieval of data packets 403 that are not compatible with data types from a data type database 404 and/or with data patterns from a data pattern database 405. In some embodiments, data management system 400 may further include a user interface 413 to issue an alert upon detection of a request for retrieval of data packets 403 that is not compatible with the privacy preference. In some embodiments, data packets 403 from the user's device 411 may be a response created as full or partial extraction(s) selected from the group consisting of any one of user's device files (permanent or temporary), user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory user's device static memory or the like.

[059] In some embodiments, data management system 400 may further include a user database 421 and/or a server database 431 for mapping of users and/or servers. Each user and/or user's device 411 using data management system 400 may be registered in user database 421 with corresponding privacy preference from privacy preference database 406, such that each user and/or user's device 411 may be linked to at least one privacy preference from privacy preference database 406. In some embodiments, server database 431 may include a list of servers 401 for communication with user devices 411. For example, a user may determine a predefine list of servers 401 for sharing of data (e.g., determine a whitelist). Thus, privacy preference database 406 may link privacy and/or sharing preferences for each user and/or server and/or data type and/or data pattern.

[060] In some embodiments, data management system 400 may perform at least one of sharing, blocking and/or modifying, per the modification algorithm 410 (e.g., such as modification algorithm 210, shown in Fig. 2), data packets 403 during communication between server 401 and user's device 411 according to the corresponding privacy preference from privacy preference database 406. For example, requests for sharing of data packets 403 of unrecognized data type may be blocked, requests for sharing of data packets 403 of allowed data type are shared, and requests for sharing of data packets 403 of forbidden data type are modified such that a predetermined response may be shared (e.g., nullify of contact data and randomly change to different mobile carrier from carrier list). In some embodiments, modification algorithm 410 may be configured for each mapped data type and/or data pattern so as to maintain communication as well as the

privacy preference by, for example randomly, modifying forbidden data packet (content) for sharing.

[061] In some embodiments, data mapping system 200 (shown in Fig. 2) may be continuously updates such that blocked unrecognized data types may be stored in a dedicated memory (such as memory 120 in Fig. 1) until this data type is mapped and recognized.

[062] In some embodiments, data management system 400 may perform at least one of sharing, blocking and modifying data packets 403 during communication between server 401 and user's device 411 in substantially real time such that the user may continue operation of user's device 411 while data management system 400 may operate in the background and/or operate in application mode for some operating systems (e.g., IOS) and/or some browsers (e.g., Safari). In some embodiments, data management system 400 (in contrast to the data-mapping stage) may handle encrypted data packets 403 since determination of data type does not read and concern the actual content of the data packet 403 even if the content is encrypted. It should be noted that while the mapping stage (e.g., described in Figs. 2 and 3A-3C) may require reading the content of the data packets for initial determination of data type and/or data pattern and/or privacy preference, the data management system 400, in contrast, does not need to read the actual content of the data packets.

[063] In some embodiments, data management system 400 may include a data pattern database 405 (such as data pattern database 205 in Fig. 2) with at least one data pattern corresponding to sharing of at least one data packet 403 (such as data packet 203 in Fig. 2) from user's device 411. In some embodiments, various data packets may be analyzed (e.g., by a processor) to determine reoccurring data patterns and thereby create data pattern database 405. As may be apparent to one of ordinary skill in the art, computerized devices such as user's device 411 may include a plurality of data packets 403 with various information (e.g., time zone, type of operating system, location, web browsing history, mouse movement, external audio, eye's focus tracking etc.) regarding the user's device 411.

[064] During communication with remote servers such as server 401, the server may send requests for sharing of these data packets 403, wherein the user's device 411 may automatically provide a corresponding response (or data packet) that is compatible with

the received request without knowledge, control and/or authorization of the user. According to some embodiments, data management system 400 may manage data packets 403 that are shared with server 401 according to a predefined privacy preference. In some embodiments, data management system 400 may further include a privacy preference database 406 (such as privacy preference database 206 in Fig. 2) with a predetermined privacy preference and/or a list of allowed and/or forbidden types of data packets 403 for sharing and/or modifying and/or, if not recognized, for blocking during communication with the at least one user's device 411. In some embodiments, at least some elements of the data management system 400 may be similar to corresponding elements in data mapping system 200, for example privacy preference database 406 while the content of data packet is not read.

[065] In some embodiments, data management system 400 may further include a communication module 412 configured to allow communication between the server 401 and the at least one user's device 411. In some embodiments, a user may determine at least one privacy preference from privacy preference database 406 with privacy preferences for data types and/or data patterns that the user allows for sharing (and/or forbidden types to be modified and/or, if not recognized types, to be blocked), for example the user may choose to block sharing of location data of any kind.

[066] In some embodiments, data management system 400 may further include a processor 402 (such as controller 105, shown in Fig. 1) coupled to the data pattern database 405 and to the privacy preference database 406. In some embodiments, processor 402 may be coupled to communication module 412. In some embodiments, processor 402 may be embedded in user's device 411. In some embodiments, processor 402 may determine at least one data pattern for sharing of data packet 403 that is for example compatible with the list of allowed types of data packets 403 from data type database 404 for sharing. In some embodiments, processor 402 may be embedded in server 401.

[067] In some embodiments, data management system 400 may operate in user's device 411 (e.g., in the form of internal proxy) to manage sharing of data packets 403, while data management system 400 may not affect other functionalities of the user's device 411 so as to allow uninterrupted usage of the device.

[068] Reference is now made to Fig. 5, which shows a flowchart for a method of management of data packets with a sharing algorithm during communication between a

remote server and a user's device, according to some embodiments of the invention. The processor (e.g., processor 402) may provide a data packet 403, for instance in response to a request for sharing of data. The received data packet 403 may be checked 501 for known or unknown element, for instance checked 501 for known data type and/or known data pattern based on data type database 404 and/or data pattern database 405. According to some embodiments, unknown elements may be determined as unrecognized and be blocked 510 by the sharing algorithm and not shared (e.g., with the server).

[069] In some embodiments, known elements may be checked 502 for allowed or forbidden elements, for instance checked 502 for allowed data type and/or allowed data pattern based on privacy preference database 406. According to some embodiments, allowed elements may be shared 520 by the sharing algorithm. According to some embodiments, forbidden elements may be, for example randomly, modified 530 by the predetermined modification algorithm 410 with sharing 520 of the modified content (e.g., with the server). For example, a user choosing not to share the country name may choose a privacy preference to modify such data packet to always share a random country name from a list of countries (e.g., "France") by modifying the data packet to be shared with the user, in order to maintain ongoing communication with the server.

[070] It should be noted that with data management system 400, the user may choose features for sharing such that other features that are forbidden for sharing may be modified so as to allow continuous and uninterrupted communication with the server.

[071] Reference is now made to Fig. 6A, which shows a flowchart for a method of dynamic management of private data during communication between a remote server 401 and a user's device 411, according to some embodiments of the invention. In some embodiments, user's device 411 may receive 601 a request for retrieval of at least one data packet 403 from the user's device 411, wherein the user's device 411 may provide a response corresponding to the received request.

[072] In some embodiments, the user's device 411 may determine 602 the data type of the at least one data packet 403 corresponding to the received request. In some embodiments, the user's device 411 may receive 603 a privacy preference for the user's device 411, wherein the privacy preference includes a list of allowed (or forbidden) data packet types for sharing (or randomly modifying per the predetermined modification algorithm for each forbidden data type) during communication. In some embodiments,

data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference may be modified 604. In some embodiments, responses to requests for sharing of data packets 403 of unrecognized type may be blocked. In some embodiments, communication between the remote server 401 and the user's device 411 may be maintained 605 with sharing of the modified data packets (e.g., responses).

[073] In some embodiments, the user's device 411 may determine a pattern of at least one response corresponding to the received request, and modify data packets (e.g., responses) to requests for sharing of data packets 403 corresponding to at least one data pattern that are not compatible with the received privacy preference. In some embodiments, the privacy preference may include a list of allowed data patterns for sharing during communication.

[074] It should be noted that such predetermined modification per each forbidden data packet type, may be a fixed or random action, depend on the user's preference and the content (e.g. nullify for password and randomly change to different country from countries list). For data packets that are not compatible with the received privacy preference (as determined by the user) may allow users to optimally control sharing of their data. For example, a user choosing not to share location data may use the system to randomly modify the data packets during communication (as above) such that the location data may not be transferred via other means (e.g., user's instruction not to share location, application blocking only sensor GPS data while sharing country code data).

[075] In some embodiments, the user's device 411 may include a database with at least one data packet type corresponding to a request for sharing of data packets 403 from the user's device 411, wherein the type of data packets 403 may be determined from the data packet type database. In some embodiments, at least one response may be linked to a type of data packet 403 from the user's device 411, wherein the linking may be based on the data type and data pattern of the at least one response.

[076] In some embodiments, a response corresponding to a request for sharing of data packets may be identified (e.g., by a processor 402), wherein the identified response is not compatible with the received privacy preference. In some embodiments, a response with at least one modified data packet corresponding to the request for sharing types of data packets may be provided per the modification algorithm. In some embodiments,

modification of the at least one modified data packet 403 may be selected from the group consisting of data nullification, change of encoding and/or file template, change of header and/or footer, blocking, data randomization, content modification, addition of a predetermined data packet, encryption or the like.

[077] In some embodiments, a communication pattern between the server 401 and the user's device 411 may be identified, wherein the communication pattern may include at least one request for retrieval of at least one data packet 403 from the user's device 411 and corresponding responses. In some embodiments, an alert may be issued (e.g., by a processor 402) upon detection of a change in the identified communication pattern. In some embodiments, data packets 403 from the user's device 411 may be a response created as full or partial extraction(s) selected from the group consisting of any one of user's device files (permanent or temporary), user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory user's device static memory or the like. .

[078] Reference is now made to Fig. 6B, which shows a flowchart for a method of dynamic management of private data during communication between a remote server 401 and a user's device 411, according to some embodiments of the invention. In some embodiments, user's device 411 may receive 611 a request for retrieval of at least one data packet 403 from the user's device 411, wherein the user's device 411 may provide a response corresponding to the received request.

[079] In some embodiments, user's device 411 may determine 612 at least one data pattern corresponding to the received request. In some embodiments, user's device 411 may receive 613 a privacy preference for the user's device 411, wherein the privacy preference may include a list of allowed (and/or forbidden) data patterns for sharing (and/or randomly modifying according to the predetermined modification algorithm for each of the forbidden data patterns) during communication. In some embodiments, responses corresponding to requests for sharing of data packets and corresponding data patterns that are not compatible with the received privacy preference may be modified 614. In some embodiments, communication between the remote server 401 and the user's device 411 may be maintained 615 with sharing of the modified responses.

[080] In some embodiments, user's device 411 may determine the type of the at least one data packet 403 of the received request. In some embodiments, requests for sharing of data

packets 403 and corresponding data patterns, corresponding to at least one data packet type, that are not compatible with the received privacy preference may be modified. In some embodiments, the privacy preference may include a list of allowed (and/or forbidden) data packet types for sharing (and/or modifying) during communication.

[081] In some embodiments, user's device 411 may include a database with at least one data pattern corresponding to a request for sharing of data packets from the user's device, and wherein the at least one data pattern compatible with the received request may be determined from the database. In some embodiments, user's device 411 may determine the type of the at least one data packet 403 of the received request, and link at least one data pattern to a type of data packet from the user's device 411, wherein the linking may be based on the pattern of the at least one response.

[082] In some embodiments, a data pattern corresponding to a request for sharing of types data packets 403 may be identified (e.g., by a processor 402), wherein the identified data pattern is not compatible with the received privacy preference. In some embodiments, a response with at least one modified data packet corresponding to the request for sharing types of data packets may be provided.

[083] In some embodiments, an alert may be issued (e.g., by a processor 402) upon detection of a request for sharing data packets, wherein the detected request does not correspond to a data type and/or a data pattern and/or a combination thereof that is not compatible with the received privacy preference. In some embodiments, a communication pattern between the server 401 and the user's device 411 may be identified, wherein the communication pattern may include at least one request for retrieval of at least one data packet 403 from the user's device 411 and corresponding responses. In some embodiments, an alert may be issued (e.g., by a processor 402) upon detection of a change in the identified communication pattern.

[084] In some embodiments, a data management system (e.g., data management system 400 as shown in Fig. 4) may be implemented as an exit gatekeeper to monitor outflow communication. For example, in network embedded devices (NED) with limited CPU power, low memory capacity and low power resources means (e.g., internet of things (IOT) device and/or machine to machine and/or machine to server communication and/or other thin client or the like). Outflow communication may be monitored for communication patterns and/or data packet type and/or data pattern and once going out of

predefined type and/or pattern range, may limit communication flow and/or block it. This ability to monitor and control outflow communication by the system may prevent for any user's device and/or NED, from being part of communication overloading attacks for example distributed denial of service (DDoS) attack or the like. Such attacks may be created by malicious attackers who are remotely using uncontrolled user's device and/or NED or the like, to generate very high communication flow (e.g., 1 terabyte per second) in short period of time (e.g. hundreds of thousands or more of IP address endpoints at the same time) that basically overload the attacked server(s) until it adversely impacts its ability to function and in some cases creates fatal malfunction in mission critical systems.

[085] Reference is now made to Fig. 7, which schematically illustrates a data management system 700 for dynamic management of private data that is at least partially embedded on a hardware component 711 (indicated with a solid line), according to some embodiments of the invention. The data management system 700 may include the communication module and/or processor adjusted and preconfigured to privacy preference methods and processes and/or data storage such as privacy preference database. The data management system 700 may be at least partially embedded on a hardware component 711, for instance embedded on one chip and/or integrated circuit and/or processor. According to some embodiments the system may communicate with server 401 and/or user's device 411 via the communication module 412. In some embodiments, the hardware component 711 (indicated with a solid line) may include at least one privacy preference database that been preconfigured and may be updated only locally so that no remote change can be made, for example by using electrically erasable programmable read-only memories (EEPROMs). In some embodiments, the hardware component 711 (indicated with a solid line) may be embedded and/or added to user's device 411 (indicated with a dashed line).

[086] For example, such data management system 700 may be added into an IOT device (e.g., adding a chip and/or a circuit to the CPU) such that DDoS may be prevented, for example, communication between the IOT device may be monitored and controlled for unusual communication patterns, such that data patterns containing higher frequency (e.g. higher than ten data packets per second) and/or data flow (e.g., higher than 1megabyte per second) may be blocked by the system, according to privacy preferences determined for that purpose. For example, as shown in Fig. 3C as well. It should be noted that such

preferences may only check data patterns where the data type of the data packets in the communication are not checked.

[087] Unless explicitly stated, the method embodiments described herein are not constrained to a particular order in time or chronological sequence. Additionally, some of the described method elements can be skipped, or they can be repeated, during a sequence of operations of a method.

[088] Various embodiments have been presented. Each of these embodiments may of course include features from other embodiments presented, and embodiments not specifically described may include various features described herein.

CLAIMS

1. A method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request;

determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request;

receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication;

modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference; and

maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

2. The method of claim 1, wherein the communication data type of the at least one data packet is determined from metadata of communication with the remote server.

3. The method of claim 1, further comprising:

determining, by the user's device, at least one communication data pattern of at least one data packet corresponding to the received request; and

modifying data packets corresponding to requests for sharing of responses corresponding to at least one data pattern, that are not compatible with the received privacy preference,

wherein the privacy preference comprises a list of allowed data patterns for sharing during communication.

4. The method of claim 1, wherein the communication data pattern is determined based on a range selected from a group consisting of: data packet frequency, data packet size, data packet speed, data packet count, data packet ratio compared to other data type flow, data packet repentance, and data packet order.

5. The method of claim 1, wherein the communication data type is determined based on data packet characteristics selected from a group consisting of: data packet header, data packet footer, version number, IP address, HTTPS, file extension, encryption method, encoding method, keywords, driver, and communication protocol.

6. The method of claim 1, wherein the user's device is in communication with an external database with at least one data packet type corresponding to a request for sharing of data packets from the user's device, and wherein the type of data packets is determined from the database.

7. The method of claim 1, further comprising:

determining, by the remote server, the communication data pattern of the at least one data packet of the received request; and

linking at least one response from the user's device to a type of data packet from the user's device, wherein the linking is based on the communication data type and communication data pattern of the at least one response.

8. The method of claim 1, further comprising:

identifying a response corresponding to a request for sharing of data packets, wherein the identified response is not compatible with the received privacy preference; and

providing a response with at least one modified data packet corresponding to the request for sharing types of data packets.

9. The method of claim 8, wherein the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

10. The method of claim 1, further comprising:

identifying a communication pattern between the server and the user's device, wherein the communication pattern comprises at least one request for retrieval of at least one data packet from the user's device and corresponding responses; and

issuing an alert upon detection of a change in the identified communication pattern.

11. The method of claim 1, wherein data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

12. A method of dynamic management of private data during communication between a remote server and a user's device, the method comprising:

receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request;

determining, by the remote server, at least one communication data pattern corresponding to the received request;

receiving, by the user's device, a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data patterns for sharing during communication;

modifying data packets corresponding to requests for sharing of responses and corresponding data patterns that are not compatible with the received privacy preference; and

maintaining communication between the remote server and the user's device, with sharing of the modified data packets.

13. The method of claim 12, wherein the communication data pattern of the at least one response is determined from metadata of communication with the remote server.

14. The method of claim 12, further comprising:

determining, by the remote server, the communication data type of the at least one data packet of the received request; and

modifying data packets corresponding to requests for sharing of responses and corresponding data patterns, corresponding to at least one communication data packet type, that are not compatible with the received privacy preference,

wherein the privacy preference comprises a list of allowed data packet types for sharing during communication.

15. The method of claim 12, wherein the communication data type is determined based on data packet characteristics selected from a group consisting of: data packet header, data packet footer, version number, IP address, HTTPS, file extension, encryption method, encoding method, keywords, driver, and communication protocol.

16. The method of claim 12, wherein the communication data pattern is determined based on a range selected from a group consisting of: data packet frequency, data packet size, data packet speed, data packet count, data packet ratio compared to other data type flow, data packet repentance, and data packet order.

17. The method of claim 12, wherein the user's device is in communication with an external database with at least one communication data pattern corresponding to a request for sharing of data packets from the user's device, and wherein the at least one data pattern compatible with the received request is determined from the database.

18. The method of claim 12, further comprising:

determining, by the remote server, the type of the at least one data packet of the received request; and

linking at least one data pattern to a type of data packet from the user's device, wherein the linking is based on the communication data type and the communication data pattern of the at least one response.

19. The method of claim 12, further comprising:

identifying a communication data pattern corresponding to a request for sharing of data packet types, wherein the identified data pattern is not compatible with the received privacy preference; and

providing a response with at least one modified data packet corresponding to the request for sharing types of data packets.

20. The method of claim 19, wherein the modification of the at least one modified data packet is selected from the group consisting of data nullification, blocking, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.

21. The method of claim 12, further comprising issuing an alert upon detection of a request for sharing data packets, wherein the detected request does not correspond to at least one of communication data type and communication data pattern that is compatible with the received privacy preference.

22. The method of claim 12, further comprising:

identifying a communication pattern between the server and the user's device, wherein the communication pattern comprises at least one request for retrieval of at least one data packet from the user's device and corresponding responses; and

issuing an alert upon detection of a change in the identified communication pattern.

23. The method of claim 12, wherein data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

24. A system for dynamic management of private data during communication between a remote server and at least one user's device, the system comprising:

a communication data type database, comprising at least one communication data type corresponding to sharing of at least one data packet from the user's device;

a privacy preference database, comprising a list of allowed types of data packets for sharing during communication with the at least one user's device;

a communication module, to allow communication between the remote server and the at least one user's device; and

a processor, coupled to the response database and to the privacy preference database,

wherein the processor is configured to instruct the remote server to determine at least one data type for sharing of data packet that is compatible with the list of allowed patterns of data packets for sharing.

25. The system of claim 24, further comprising a user interface to issue an alert upon detection of a request for retrieval of data packets that is not compatible with the privacy preference.

26. The system of claim 24, further comprising a communication data pattern database, coupled to the processor and comprising at least one data pattern corresponding to sharing of at least one data packet from the user's device, wherein the processor is configured to modify data packets corresponding to requests for retrieval of data packets and communication data types that are not compatible with communication data patterns from a communication data pattern database.

27. The system of claim 26, wherein data packets from the user's device are selected from the group consisting of user's device files, user's device characteristics, user's device indirect attributes, user's device sensor data, user's device browser data, user's device form data, user's device dynamic memory and user's device static memory.

28. The system of claim 26, wherein at least the communication module and the processor are embedded on a single hardware component.

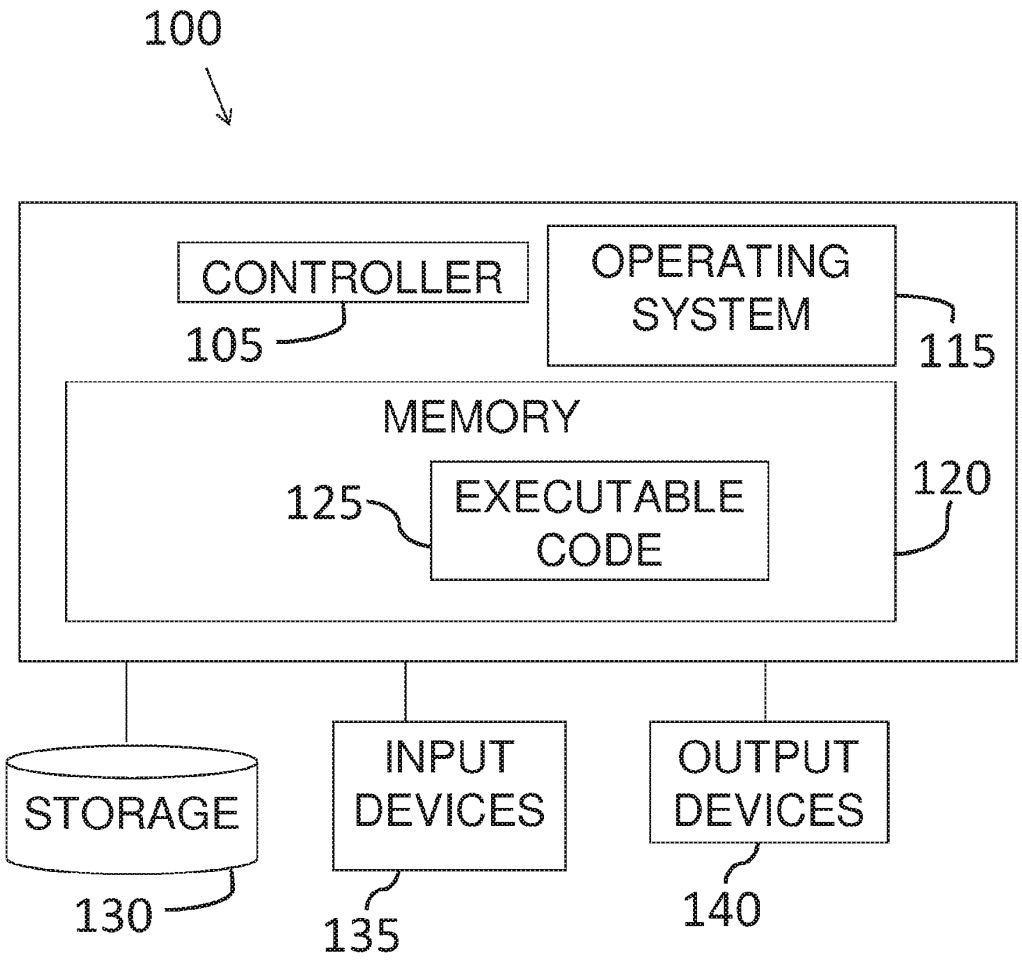

100
CONTROLLER
105
OPERATING SYSTEM
115
MEMORY
125
EXECUTABLE CODE
120
STORAGE
130
INPUT DEVICES
135
OUTPUT DEVICES
140

Fig. 1

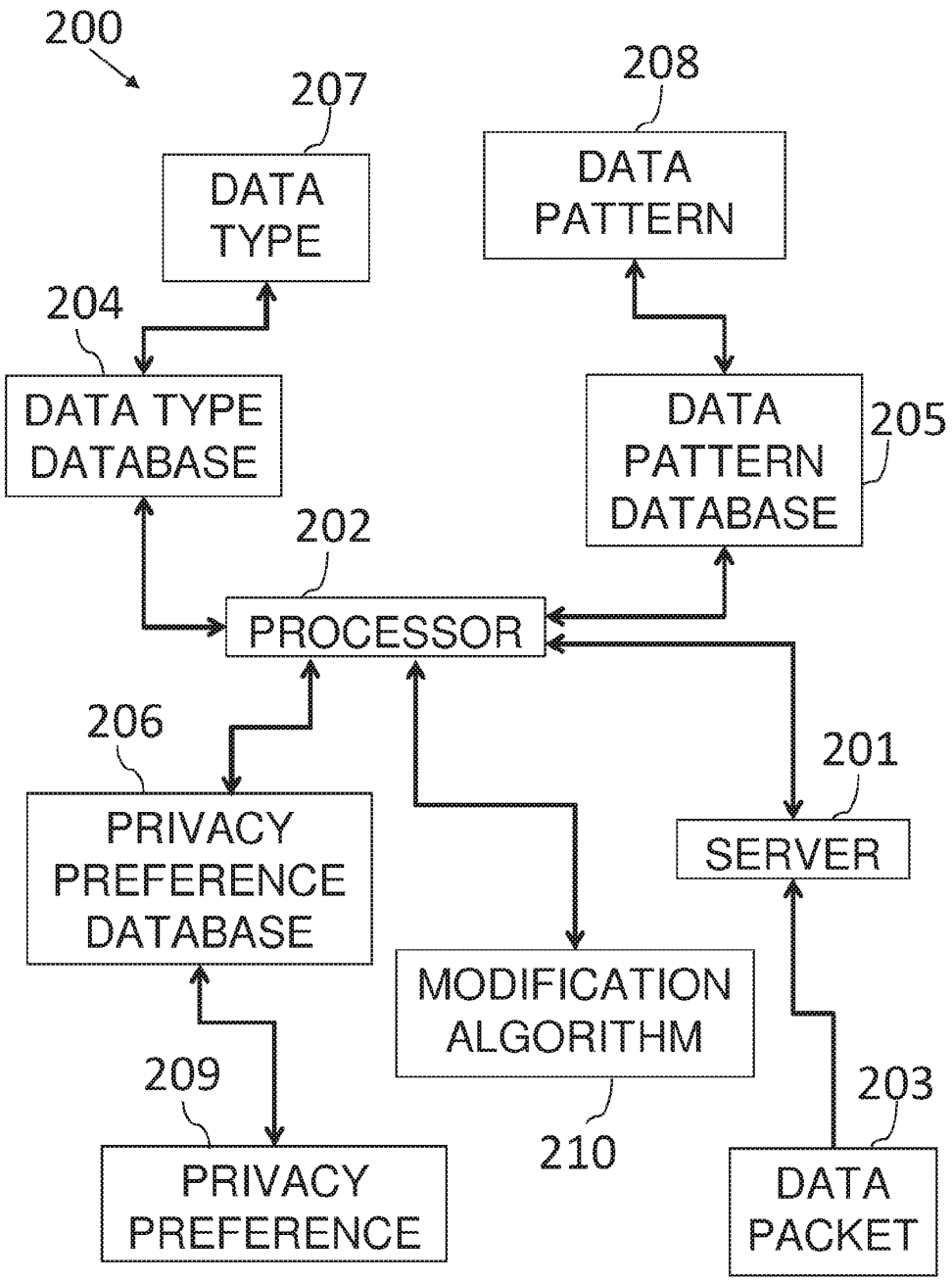

200
207
DATA TYPE
208
DATA PATTERN
204
DATA TYPE DATABASE
DATA PATTERN DATABASE
205
202
PROCESSOR
206
201
PRIVACY PREFERENCE DATABASE
SERVER
MODIFICATION ALGORITHM
209
203
210
PRIVACY PREFERENCE
DATA PACKET

Fig. 2

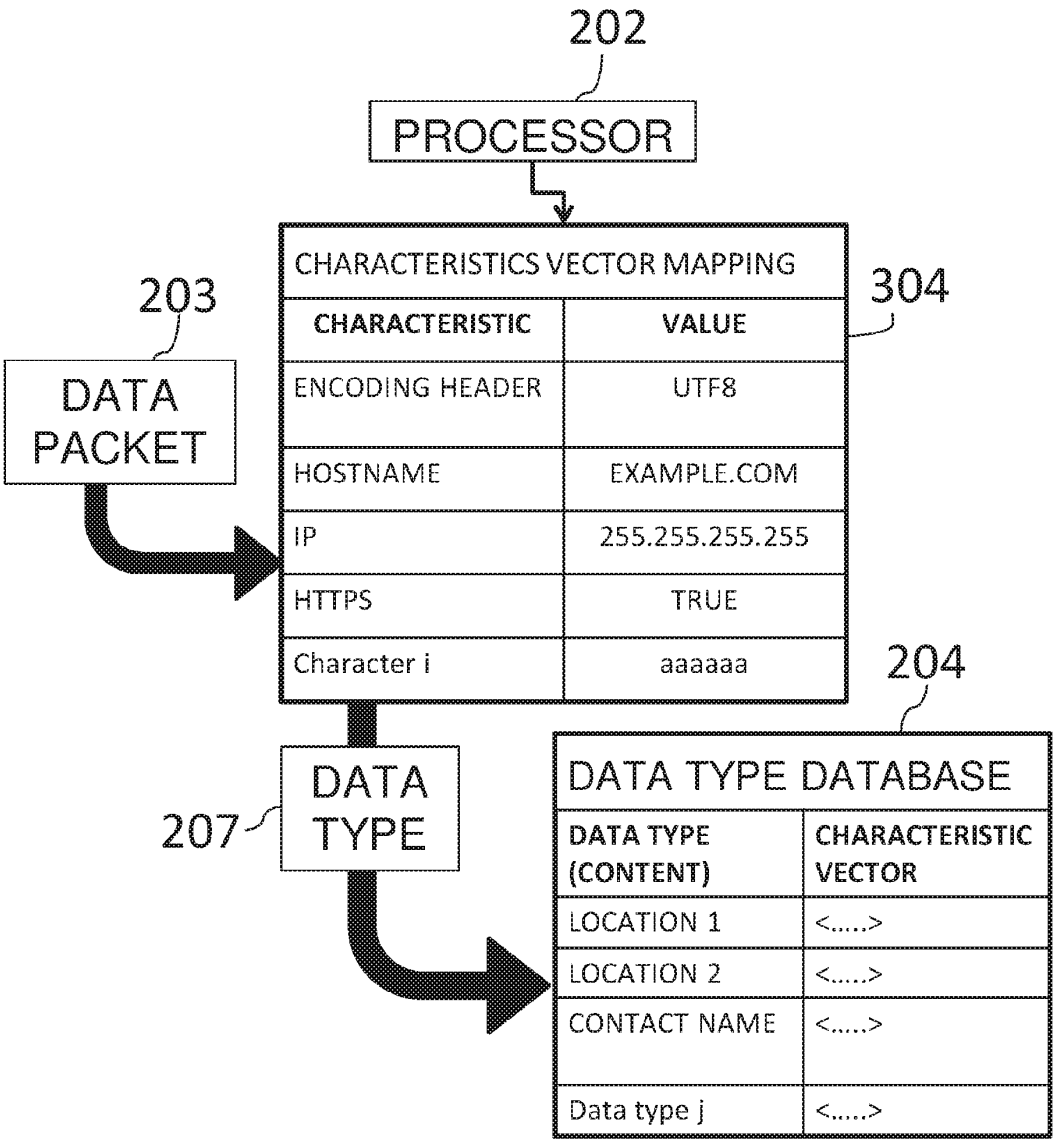

202
PROCESSOR
203
DATA PACKET
CHARACTERISTICS VECTOR MAPPING
304
CHARACTERISTIC
VALUE
ENCODING HEADER
UTF8
HOSTNAME
EXAMPLE.COM
IP
255.255.255.255
HTTPS
TRUE
Character i
aaaaaa
204
207
DATA TYPE
DATA TYPE DATABASE
DATA TYPE (CONTENT)
CHARACTERISTIC VECTOR
LOCATION 1
<.....>
LOCATION 2
<.....>
CONTACT NAME
<.....>
Data type j
<.....>

Fig.3A

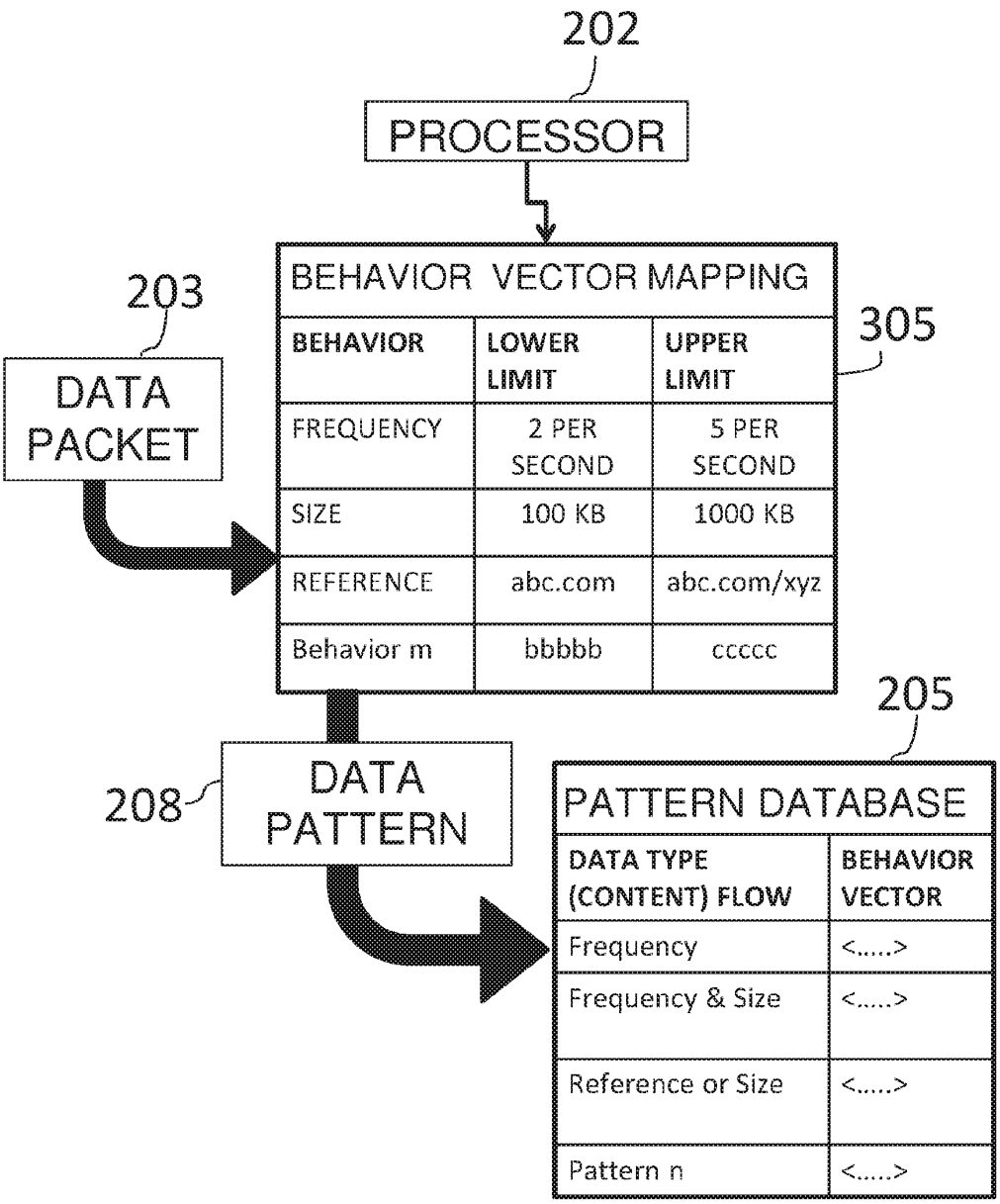
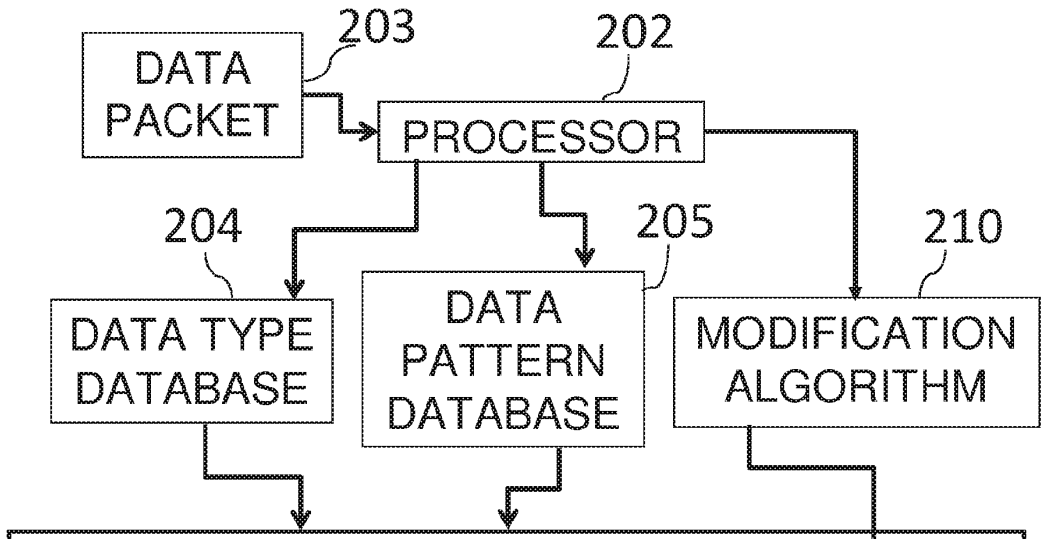

202
PROCESSOR
203
DATA PACKET
BEHAVIOR VECTOR MAPPING
305
BEHAVIOR
LOWER LIMIT
UPPER LIMIT
FREQUENCY
2 PER SECOND
5 PER SECOND
SIZE
100 KB
1000 KB
REFERENCE
abc.com
abc.com/xyz
Behavior m
bbbbb
ccccc
205
208
DATA PATTERN
PATTERN DATABASE
DATA TYPE (CONTENT) FLOW
BEHAVIOR VECTOR
Frequency
<.....>
Frequency & Size
<.....>
Reference or Size
<.....>
Pattern n
<.....>

Fig. 3B



PRIVACY PREFERENCE TABLE

Data Type (content)	Data Type	Data Pattern	Modification Strategy
Audio	<.....>	Low Frequency	Change File's Template
Location 3 (country)	<.....>	Low Frequency & Small Size	Random change - from list of countries
Contact Name	<.....>	Any Pattern	Random change - from list of dummy contacts
Password	<.....>	No Pattern checked	Nullify value
No datatype checked	Any type	Frequency limit or flow limit	Reduce to limitations, if repeat than Block
...	...	...	...

306

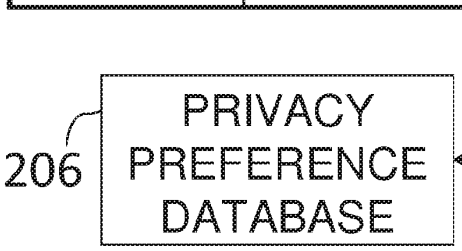


Fig. 3C

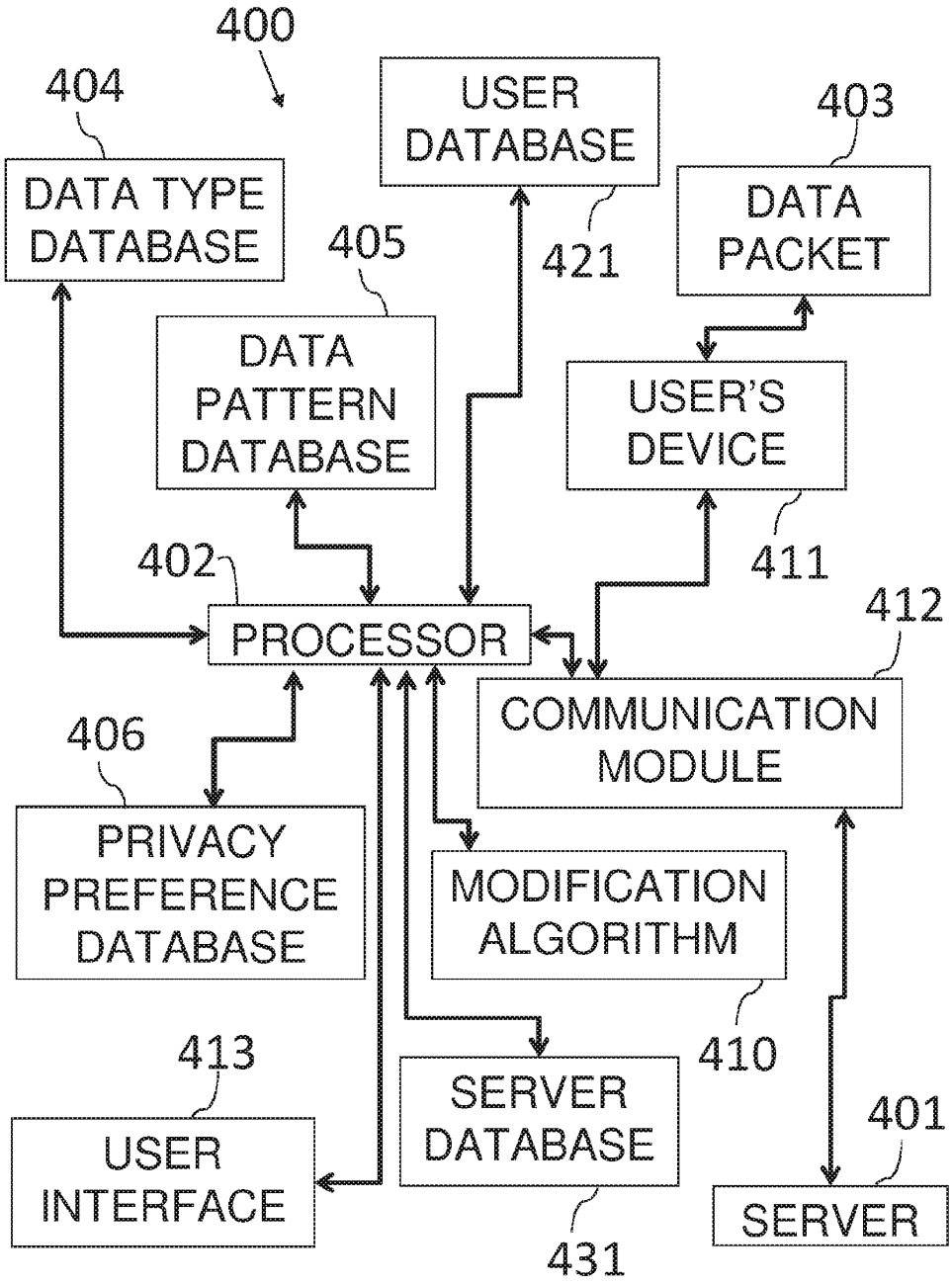

400
404
DATA TYPE DATABASE
USER DATABASE
421
403
DATA PACKET
405
DATA PATTERN DATABASE
USER'S DEVICE
411
402
PROCESSOR
412
COMMUNICATION MODULE
406
PRIVACY PREFERENCE DATABASE
MODIFICATION ALGORITHM
410
413
USER INTERFACE
SERVER DATABASE
431
401
SERVER

Fig. 4

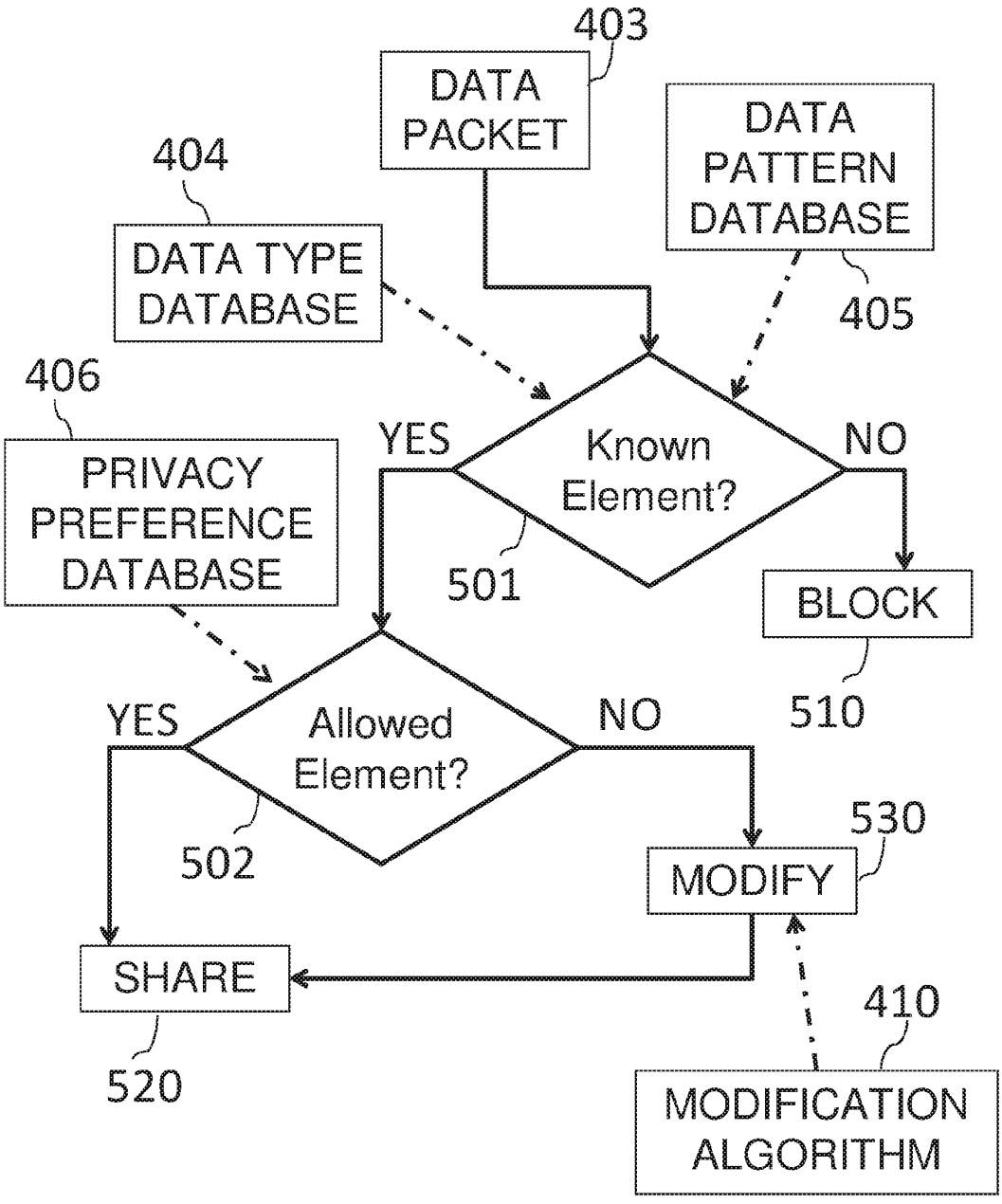

403
DATA PACKET
DATA PATTERN DATABASE
404
DATA TYPE DATABASE
405
406
PRIVACY PREFERENCE DATABASE
YES
Known Element?
NO
501
BLOCK
510
YES
Allowed Element?
NO
502
530
MODIFY
SHARE
520
410
MODIFICATION ALGORITHM

Fig. 5

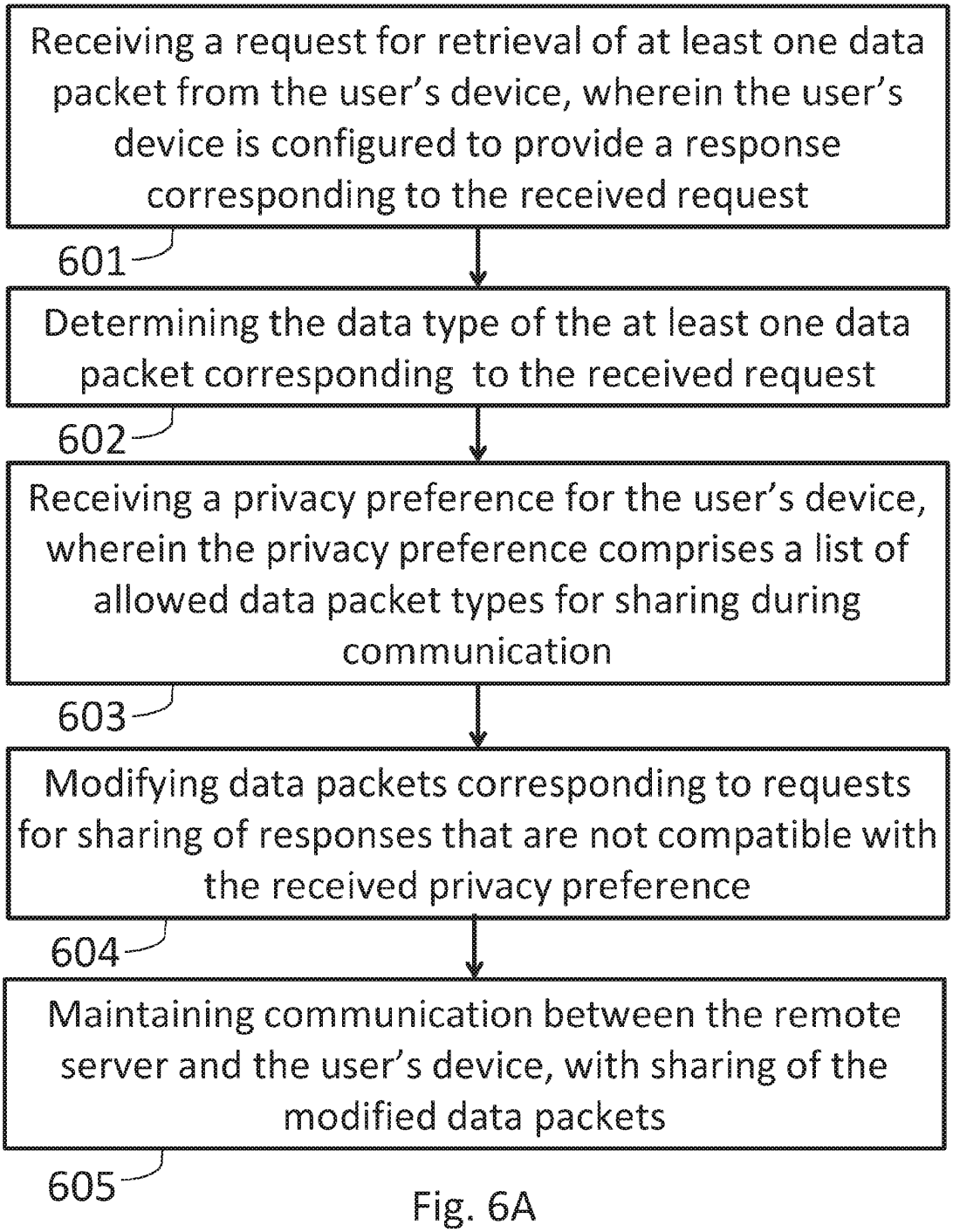

Receiving a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request
601
Determining the data type of the at least one data packet corresponding to the received request
602
Receiving a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data packet types for sharing during communication
603
Modifying data packets corresponding to requests for sharing of responses that are not compatible with the received privacy preference
604
Maintaining communication between the remote server and the user's device, with sharing of the modified data packets
605

Fig. 6A

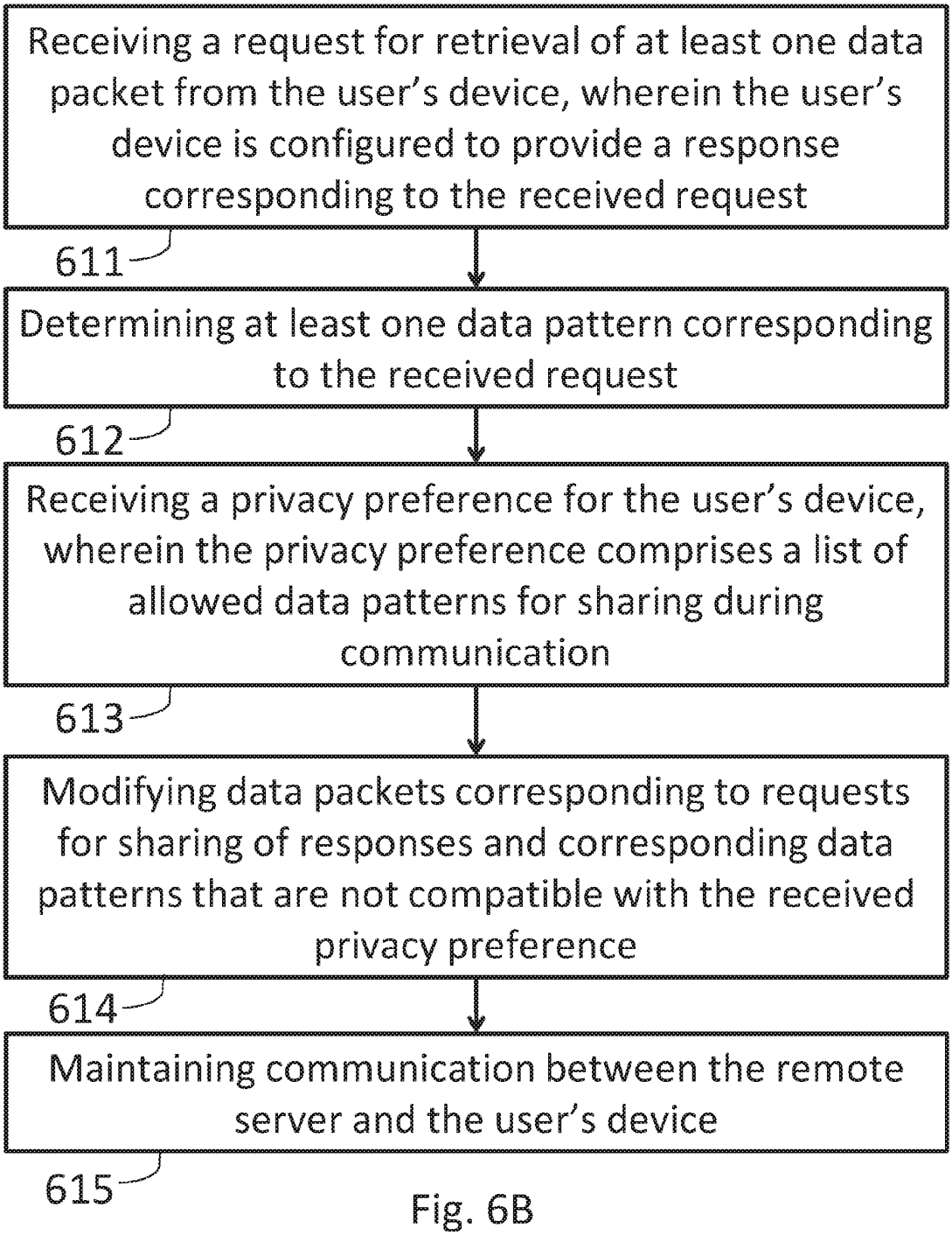

Receiving a request for retrieval of at least one data packet from the user's device, wherein the user's device is configured to provide a response corresponding to the received request
611
Determining at least one data pattern corresponding to the received request
612
Receiving a privacy preference for the user's device, wherein the privacy preference comprises a list of allowed data patterns for sharing during communication
613
Modifying data packets corresponding to requests for sharing of responses and corresponding data patterns that are not compatible with the received privacy preference
614
Maintaining communication between the remote server and the user's device
615

Fig. 6B

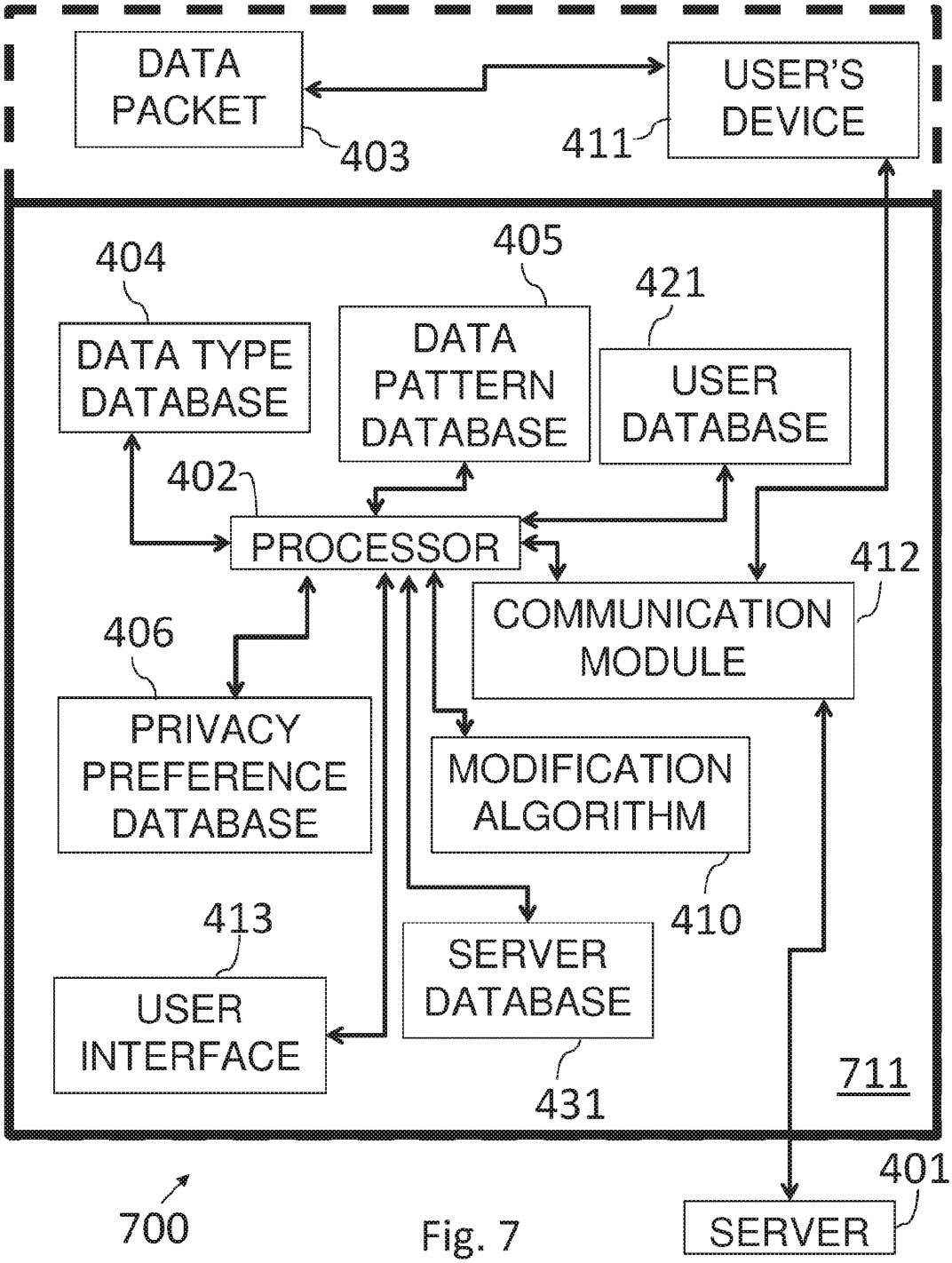

DATA PACKET
403
USER'S DEVICE
411
404
DATA TYPE DATABASE
405
DATA PATTERN DATABASE
421
USER DATABASE
402
PROCESSOR
412
COMMUNICATION MODULE
406
PRIVACY PREFERENCE DATABASE
MODIFICATION ALGORITHM
410
413
USER INTERFACE
SERVER DATABASE
431
711
401
SERVER
700

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2018/050359

A. CLASSIFICATION OF SUBJECT MATTER
IPC (2018.01) H04L 29/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC (2018.01) H04L 29/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Databases consulted: Esp@cenet, Google Patents
Search terms used: privacy communication data type and communication data pattern of "data packet";

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013318347 A1 MOFFAT BRIAN LEE?[US] 28 Nov 2013 (2013/11/28) ¶ 78, 149, 221, 232, 494, 499-501, 804	1-28

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"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)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 Jul 2018	12 Jul 2018
Name and mailing address of the ISA: Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Facsimile No. 972-2-5651616	Authorized officer MARCOWITZ Noam Telephone No. 972-2-5651735

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IL2018/050359

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
US 2013318347 A1	28 Nov 2013	US 2013318347 A1	28 Nov 2013
		US 9015281 B2	21 Apr 2015
		CA 2813758 A1	12 Apr 2012
		EP 2625820 A1	14 Aug 2013
		EP 2625820 A4	27 May 2015
		US 2015180839 A1	25 Jun 2015
		US 9397983 B2	19 Jul 2016
		US 2017054674 A1	23 Feb 2017
		WO 2012048347 A1	12 Apr 2012

Form PCT/ISA/210 (patent family annex) (January 2015)

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
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 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)

Attorney Docket No: P-566702-US

Title of Invention	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number PCT/IL2018/050359 filed on March 28, 2018.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application

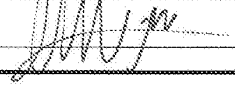
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

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.

LEGAL NAME OF INVENTOR

Inventor: Yehonatan WASSERMAN (Date Optional): 03/10/2019

Signature: 

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.

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.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
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 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)

Attorney Docket No: P-566702-US

Title of Invention	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number PCT/IL2018/050359 filed on March 28, 2018.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application

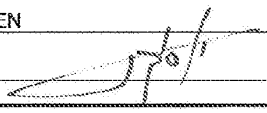
I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

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.

LEGAL NAME OF INVENTOR

Inventor: Yoseph KOREN (Date Optional): 03/10/2019

Signature: 

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.

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Yoseph KOREN et al.	Examiner:	Not yet assigned
Serial No.:	Not yet assigned	Group Art Unit:	Not yet assigned
Filed:	Herewith	Confirmation No.:	Not yet assigned
Title:	SYSTEM AND METHOD FOR DYNAMIC MANAGEMENT OF PRIVATE DATA		

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

Sir/Madam:

INFORMATION DISCLOSURE STATEMENT

Pursuant to 37 C.F.R. §§1.56, 1.97 and 1.98, this Information Disclosure Statement includes Form PTO/SB/08:

1. ☒ listing documents including patents, publications and other information for consideration by the Examiner, however, since the subject application was filed after June 30, 2003, copies of United States patents and/or United States patent application publications are not included in this information disclosure statement; and/or
2. ☐ listing documents including patents, publications and other information that have been previously cited or submitted to the Patent Office in prior application U.S. Patent application No. , filed which is properly identified and relied on for an earlier effective filing date under 35 U.S.C. 120 for consideration by the Examiner; however, in accordance with 37 C.F.R. 1.98(d), copies of such documents are not included in this information disclosure statement; and/or
3. ☐ listing documents including patents, publications, and other information for consideration by the Examiner, copies of which are included with this information disclosure statement;
4. ☒ listing documents including patents, publications, and other information for consideration by the Examiner, which were cited in a communication from a foreign patent office in a counterpart foreign application, copies of which are included with this information disclosure statement.

The information herein cited is only in fulfillment of Applicant(s) duty of candor in disclosing all information brought to Applicant(s) attention. This submission does not represent that a search has been made or that no better art exists and does not constitute an admission that each or all of the listed documents are material or constitute "prior art". If it should be determined that any of the listed documents do not constitute "prior art" under United States law, Applicant(s) reserve the right to present to the office the relevant facts and law regarding the appropriate status of such documents.

Applicant(s) further reserve(s) the right to take appropriate action to establish the patentability of the disclosed invention over the listed documents, should one or more of the documents be applied against the claims of the present application.

In accordance with MPEP Sections 609 and 707.05(b), it is requested that each and every document cited (including any cited in applicant's specification which is not repeated on the attached Form PTO-1449) be given thorough consideration and that it be cited of record in the prosecution history of the present application by initialing on Form PTO-1449. Such initialing is requested even if the Examiner does not consider it to be prior art for any reason, or even if the Examiner does not believe that the guidelines for citation have been fully complied with. This is requested so that each document becomes listed on the face of the patent issuing on the present application and is evidence that the Examiner has considered the document. Neither the submission of the Information Disclosure Statement nor the content of any document cited herein constitutes a disclaimer of claim scope or an admission that any item submitted constitutes prior art.

This Information Disclosure Statement is being filed:

I) ☒ Within three (3) months of filing the subject Application or entry of the subject Application into the national stage; or before mailing of the first Office Action on the merits of the subject Application, whichever event occurs last; or before mailing of the first Office Action on the merits after filing a request for continued examination, pursuant to of 37 C.F.R §1.97 (b); or

II) ☐ After the period specified in (I) but before the mailing date of either a final Official Action under 37 C.F.R §1.113 or a notice of allowance under 37 C.F.R §1.311 whichever occurs first and;

1. ☐ the undersigned hereby states that each item of information listed on the Form PTO-1449 was either (i) cited in a communication from a foreign patent office in a counterpart foreign application not more than three (3) months prior to the filing of this Information Disclosure Statement or (ii) not cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the undersigned after making reasonable inquiry, not known to any individual designated in §1.56(c) more than three (3) months prior to the filing of this information disclosure statement; or

2. ☐ the fee in the amount of $240 (Large Entity) under 37 C.F.R §1.17 (p) is being paid by credit card (note deposit account information below in the event of lack of credit card payment).

III) ☐ After the period in (I) and (II) but before the payment of the issue fee and,

1. The undersigned hereby states:

a) ☐ that each item of information cited on the form PTO-1449 was first cited in a communication from a foreign Patent Office in a counterpart foreign

application not more than three (3) months prior to the filing of this Information Disclosure Statement; or

b) ☐ that no items of information contained in Form PTO-1449 were cited in a communication from a foreign patent office in a counterpart foreign application, and to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in this Information Disclosure Statement was known to any individual designated in 37 C.F.R. § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement; and

2. ☐ The Petition fee in the amount of $240 (Large Entity) under 37 C.F.R §1.17 is being paid by credit card (note deposit account information below in the event of lack of credit card payment).

To the extent that there are any fees associated with this filing that are due but are not paid or are not able to be paid by a credit card mentioned elsewhere in this document, Applicants authorize the U.S. Patent and Trademark Office to charge any such fees to deposit account No. **60-2041**.

Respectfully submitted,

/Devorah Livneh, Reg. No. 71,347/
Devorah N. Livneh
Attorney/Agent for Applicant(s)
Registration No. 71,347

Dated: October 7, 2019

Pearl Cohen Zedek Latzer Baratz LLP
1500 Broadway, 12th Floor
New York, New York 10036
Tel: (646) 878-0800
Fax: (646) 878-0801