Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2975441 A1 2016/08/11

(21) 2 975 441

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) **Date de dépôt PCT/PCT Filing Date:** 2016/02/02
(87) **Date publication PCT/PCT Publication Date:** 2016/08/11
(85) **Entrée phase nationale/National Entry:** 2017/07/28
(86) **N° demande PCT/PCT Application No.:** US 2016/016143
(87) **N° publication PCT/PCT Publication No.:** 2016/126690
(30) **Priorités/Priorities:** 2015/02/06 (US62/112,654); 2015/02/20 (US62/118,612); 2015/03/03 (US62/127,824); 2015/04/27 (US62/153,392); 2015/04/28 (US62/154,049); 2015/05/14 (US62/161,408); 2015/05/20 (US62/164,013); 2015/06/12 (US62/174,527); 2015/06/19 (US62/181,772); 2015/06/23 (US62/183,606); 2015/07/07 (US62/189,237); 2015/07/16 (US62/193,127); 2015/07/31 (US62/199,292); 2015/08/11 (US62/203,424); ...

(51) **Cl.Int./Int.Cl.** ***G06F 21/60*** (2013.01), ***G06F 21/62*** (2013.01)

(71) **Demandeur/Applicant:**
ANONOS INC., US

(72) **Inventeurs/Inventors:**
LAFEVER, MALCOLM GARY, US;
MYERSON, TED N., US;
MASON, STEVEN, US

(74) **Agent:** RICHES, MCKENZIE & HERBERT LLP

(54) **Titre : SYSTEMES ET PROCEDES POUR LA PROTECTION DE DONNEES CONTEXTUALISEES**
(54) **Title: SYSTEMS AND METHODS FOR CONTEXTUALIZED DATA PROTECTION**

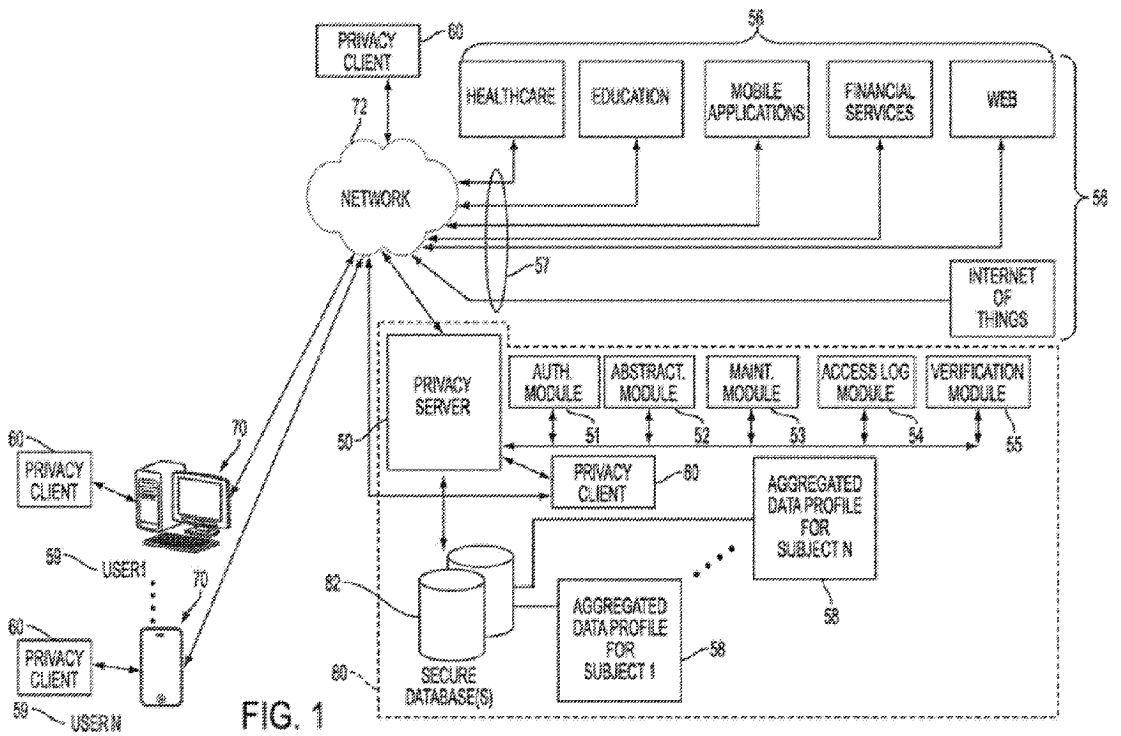

FIG. 1

(57) **Abrégé/Abstract:**
Various systems, computer-readable media, and computer-implemented methods of providing improved data privacy, anonymity, and security by enabling subjects to which data pertains to remain "dynamically anonymous," i.e., anonymous for as long as is desired→ and to the extent that is desired→ are disclosed herein. This concept is also referred to herein as Just-In-Time-Identity, or "JITI." Embodiments include systems that create, access, use, store and / or erase data with increased privacy, anonymity and security→ thereby facilitating the availability of more qualified information→ via the use of temporally unique, dynamically changing de-identifiers ("DDIDs"). In some embodiments, specialized JITI keys may be used to "unlock" different views of the same DDID (or its underlying value), thereby providing granular control over the level of detail or obfuscation visible to each user based on the context of said user's authorized use of data, e.g., authorized purpose(s), place(s), time(s), or other attributes of the use.

(21) **2 975 441**

(13) **A1**

(30) **Priorités(suite)/Priorities(continued):** 2015/08/27 (US62/210,457); 2015/09/04 (US14/846,167)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 August 2016 (11.08.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/126690 A1

(51) **International Patent Classification**:
G06F 21/62 (2013.01)

(21) **International Application Number**:
PCT/US2016/016143

(22) **International Filing Date**:
2 February 2016 (02.02.2016)

(25) **Filing Language**: English

(26) **Publication Language**: English

(30) **Priority Data**:

62/112,654	6 February 2015 (06.02.2015)	US
62/118,612	20 February 2015 (20.02.2015)	US
62/127,824	3 March 2015 (03.03.2015)	US
62/153,392	27 April 2015 (27.04.2015)	US
62/154,049	28 April 2015 (28.04.2015)	US
62/161,408	14 May 2015 (14.05.2015)	US
62/164,013	20 May 2015 (20.05.2015)	US
62/174,527	12 June 2015 (12.06.2015)	US
62/181,772	19 June 2015 (19.06.2015)	US
62/183,606	23 June 2015 (23.06.2015)	US
62/189,237	7 July 2015 (07.07.2015)	US
62/193,127	16 July 2015 (16.07.2015)	US
62/199,292	31 July 2015 (31.07.2015)	US
62/203,424	11 August 2015 (11.08.2015)	US
62/210,457	27 August 2015 (27.08.2015)	US
14/846,167	4 September 2015 (04.09.2015)	US

(71) **Applicant**: **ANONOS INC.** [US/US]; 228 Park Ave. South, Suite 96049, New York, NY 10003-1502 (US).

(72) **Inventors**: **LAFEVER, Malcolm, Gary**; 228 Park Ave. South, Suite 96049, New York, NY 10003-1502 (US). **MYERSON, Ted N.**; 228 Park Ave. South, Suite 96049, New York, NY 10003-1502 (US). **MASON, Steven**; 228 Park Ave. South, Suite 96049, New York, NY 10003-1502 (US).

(74) **Agent**: **PETERSON, Daniel, R.**; Blank Rome LLP, 717 Texas Avenue, Suite 1400, Houston, TX 77002 (US).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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**: SYSTEMS AND METHODS FOR CONTEXTUALIZED DATA PROTECTION

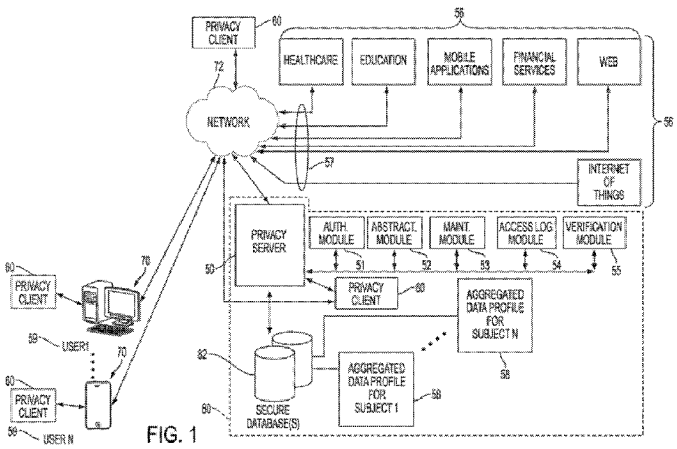

FIG. 1

(57) **Abstract**: Various systems, computer-readable media, and computer-implemented methods of providing improved data privacy, anonymity, and security by enabling subjects to which data pertains to remain "dynamically anonymous," i.e., anonymous for as long as is desired— and to the extent that is desired— are disclosed herein. This concept is also referred to herein as Just-In-Time-Identity, or "JITI." Embodiments include systems that create, access, use, store and / or erase data with increased privacy, anonymity and security— thereby facilitating the availability of more qualified information— via the use of temporally unique, dynamically changing de-identifiers ("DDIDs"). In some embodiments, specialized JITI keys may be used to "unlock" different views of the same DDID (or its underlying value), thereby providing granular control over the level of detail or obfuscation visible to each user based on the context of said user's authorized use of data, e.g., authorized purpose(s), place(s), time(s), or other attributes of the use.

WO 2016/126690 A1

CLAIMS

1. A system, comprising:

a communication interface for sending data over a network;

a memory having, stored therein, computer program code;

and one or more processing units operatively coupled to the memory and configured to execute instructions in the computer program code that cause the one or more processing units to:

generate one or more dynamically-changing, temporally unique identifiers;

receive, over the network, a first request from a first data subject for a generated dynamically-changing, temporally unique identifier to be related to an attribute of the first data subject;

associate, in response to the first request, a first generated dynamically-changing, temporally unique identifier with the attribute of the first data subject;

transform the value of the first generated dynamically-changing, temporally unique identifier into a first unintelligible form,

wherein a first key may be used to transform the first unintelligible form back into a first view of the first generated dynamically-changing, temporally unique identifier,

wherein a second key may be used to transform the first unintelligible form back into a second view of the first generated dynamically-changing, temporally unique identifier,

wherein the first key is different from the second key, and

wherein the first view is different from the second view;

store, in the memory, the first generated dynamically-changing, temporally unique identifier, the first key, the second key, and the first unintelligible form; and

send the first unintelligible form over the network to the first data subject.

2. The system of claim 1, wherein the first view provides more detail than the second view.

3. The system of claim 1, wherein the unintelligible form comprises encrypted text.

4. The system of claim 1, wherein the instructions in the computer program code further comprise instructions that cause the one or more processing units to also associate the first generated dynamically-changing, temporally unique identifier with an attribute of a second data subject.

5. The system of claim 4, wherein the instructions in the computer program code that cause the one or more processing units to also associate the first generated dynamically-changing, temporally unique identifier with an attribute of a second data subject are executed in at least one of the following situations:

at a different time than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject;

at a different physical or virtual location than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject; and

for a different purpose than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject.

6. The system of claim 1, wherein the instructions in the computer program code further comprise instructions that cause the one or more processing units to:

associate a second generated dynamically-changing, temporally unique identifier with the attribute of the first data subject.

7. The system of claim 6, wherein the instructions in the computer program code that cause the one or more processing units to associate the second generated

dynamically-changing, temporally unique identifier with the attribute of the first data subject are executed in at least one of the following situations:

at a different time than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject;

at a different physical or virtual location than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject; and

for a different purpose than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject.

8. A non-transitory computer readable medium comprising computer executable instructions stored thereon to cause one or more processing units to:

generate one or more dynamically-changing, temporally unique identifiers;

receive, over a network, a first request from a first data subject for a generated dynamically-changing, temporally unique identifier to be related to an attribute of the first data subject;

associate, in response to the first request, a first generated dynamically-changing, temporally unique identifier with the attribute of the first data subject;

transform the value of the first generated dynamically-changing, temporally unique identifier into a first unintelligible form,

wherein a first key may be used to transform the first unintelligible form back into a first view of the first generated dynamically-changing, temporally unique identifier,

wherein a second key may be used to transform the first unintelligible form back into a second view of the first generated dynamically-changing, temporally unique identifier,

wherein the first key is different from the second key, and

wherein the first view is different from the second view;

store, in a memory, the first generated dynamically-changing, temporally unique identifier, the first key, the second key, and the first unintelligible form; and

send the first unintelligible form over the network to the first data subject.

9. The non-transitory computer readable medium of claim 8, wherein the first view provides more detail than the second view.

10. The non-transitory computer readable medium of claim 8, wherein the unintelligible form comprises non-encrypted text.

11. The non-transitory computer readable medium of claim 8, wherein the instructions further comprise instructions that cause the one or more processing units to also associate the first generated dynamically-changing, temporally unique identifier with an attribute of a second data subject.

12. The non-transitory computer readable medium of claim 11, wherein the instructions that cause the one or more processing units to also associate the first generated dynamically-changing, temporally unique identifier with an attribute of a second data subject are executed in at least one of the following situations:

at a different time than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject;

at a different physical or virtual location than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject; and

for a different purpose than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject.

13. The non-transitory computer readable medium of claim 8, wherein the instructions further comprise instructions that cause the one or more processing units to:

associate a second generated dynamically-changing, temporally unique identifier with the attribute of the first data subject.

14. The non-transitory computer readable medium of claim 13, wherein the instructions that cause the one or more processing units to associate the second generated dynamically-changing, temporally unique identifier with the attribute of the first data subject are executed in at least one of the following situations:

at a different time than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject;

at a different physical or virtual location than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject; and

for a different purpose than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject.

15. A computer-implemented method comprising:

generating one or more dynamically-changing, temporally unique identifiers;

receiving, over a network, a first request from a first data subject for a generated dynamically-changing, temporally unique identifier to be related to an attribute of the first data subject;

associating, in response to the first request, a first generated dynamically-changing, temporally unique identifier with the attribute of the first data subject;

transforming the value of the first generated dynamically-changing, temporally unique identifier into a first unintelligible form,

wherein a first key may be used to transform the first unintelligible form back into a first view of the first generated dynamically-changing, temporally unique identifier,

wherein a second key may be used to transform the first unintelligible form back into a second view of the first generated dynamically-changing, temporally unique identifier,

wherein the first key is different from the second key, and

wherein the first view is different from the second view;

storing, in a memory, the first generated dynamically-changing, temporally unique identifier, the first key, the second key, and the first unintelligible form; and

sending the first unintelligible form over the network to the first data subject.

16. The computer-implemented method of claim 15, wherein the first view provides more detail than the second view.

17. The computer-implemented method of claim 15, further comprising also associating the first generated dynamically-changing, temporally unique identifier with an attribute of a second data subject.

18. The computer-implemented method of claim 17, wherein the act of also associating the first generated dynamically-changing, temporally unique identifier with an attribute of a second data subject is performed in at least one of the following situations:

at a different time than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject;

at a different physical or virtual location than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject; and

for a different purpose than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject.

19. The computer-implemented method of claim 15, further comprising:

associating a second generated dynamically-changing, temporally unique identifier with the attribute of the first data subject.

20. The computer-implemented method of claim 19, wherein act of associating the second generated dynamically-changing, temporally unique identifier with the attribute of the first data subject is performed in at least one of the following situations:

at a different time than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject;

at a different physical or virtual location than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject; and

for a different purpose than the first generated dynamically-changing, temporally unique identifier is associated with the attribute of the first data subject.