(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 063 691 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
11.03.2020 Bulletin 2020/11

(21) Application number: **14858404.8**

(22) Date of filing: **31.10.2014**

(51) Int Cl.:
G06F 21/00 *(2013.01)* ***G06F 21/62*** *(2013.01)*
H04L 29/06 *(2006.01)*

(86) International application number:
PCT/US2014/063520

(87) International publication number:
WO 2015/066523 (07.05.2015 Gazette 2015/18)

(54) DYNAMIC DE-IDENTIFICATION AND ANONYMITY

DYNAMISCHE ENTIDENTIFIKATION UND ANONYMITÄT

DÉSIDENTIFICATION ET ANONYMAT DYNAMIQUES

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority:
01.11.2013 US 201361899096 P
11.02.2014 US 201461938631 P
18.02.2014 US 201461941242 P
25.02.2014 US 201461944565 P
27.02.2014 US 201461945821 P
06.03.2014 US 201461948575 P
23.03.2014 US 201461969194 P
03.04.2014 US 201461974442 P
05.05.2014 US 201461988373 P
13.05.2014 US 201461992441 P
15.05.2014 US 201461994076 P
16.05.2014 US 201461994721 P
16.05.2014 US 201461994715 P
21.05.2014 US 201462001127 P
21.06.2014 US 201462015431 P
02.07.2014 US 201462019987 P
15.08.2014 US 201462037703 P
28.08.2014 US 201462043238 P
03.09.2014 US 201462045321 P
16.09.2014 US 201462051270 P
26.09.2014 US 201462055669 P
04.10.2014 US 201462059882 P

(43) Date of publication of application:
07.09.2016 Bulletin 2016/36

(73) Proprietor: **Anonos Inc.**
Beaverton, OR 97008 (US)

(72) Inventors:
- **LAFEVER, Malcolm, Gary**
  New York, NY 10003-1502 (US)
- **MYERSON, Ted, N.**
  New York, NY 10003-1502 (US)
- **HAMPTON, Samantha, L.**
  New York, NY 10003-1502 (US)
- **KAUSHANSKY, Howard**
  New York, NY 10003-1502 (US)
- **MASON, Steven**
  New York, NY 10003-1502 (US)

(74) Representative: **Rooney, John-Paul**
Withers & Rogers LLP
4 More London Riverside
London SE1 2AU (GB)

(56) References cited:
WO-A1-2013/097886
DE-A1- 19 638 072
US-A1- 2004 153 908
US-A1- 2008 195 965
US-A1- 2010 199 356
US-A1- 2011 010 563
US-A1- 2011 302 598
US-A1- 2012 047 530

EP 3 063 691 B1

Description

Field of the Invention

[0001] This disclosure relates generally to improving data security, privacy, and accuracy, and, in particular, to using dynamically changing identifiers to render elements of data anonymous.

Background

[0002] This section is intended to provide a background or context to the invention that is recited in the claims. The description herein may include concepts that could be pursued, but are not necessarily ones that have been previously conceived, implemented or described. Therefore, unless otherwise indicated herein, what is described in this section is not prior art to the description and claims in this application and is not admitted to be prior art by inclusion in this section.

[0003] There are certain inherent conflicts between: (i) the goal of parties to maximize the value of data and their goal of respecting privacy rights of individuals; (ii) the goal of individuals' to protect their privacy rights and their goal of benefiting from highly personalized offerings; and (iii) the goal of U.S. and international government agencies to facilitate research and commerce and their goal of safeguarding rights of citizens.

[0004] One goal of non-healthcare-related parties is to reach the most "highly qualified" prospects, i.e., prospective buyers who have the requisite financial resources, motivation, and authority to make a purchase. Commercial parties will pay much more to reach qualified prospects than to reach undifferentiated prospects because the chances of consummating a transaction with a qualified prospect is significantly higher, given their interest, predisposition, and means to close transactions. The level of personalization / customization of offerings for prospective customers - which is directly related to the likelihood of consummating transactions - is enhanced by the depth and scope of information available about each individual prospect. One goal of healthcare-related parties is to conduct research pertaining to health and / or disease with the goal of advancing discoveries in applications that may improve human health.

[0005] The development, emergence and widespread adoption of computer networks, internets, intranets and supporting technologies has resulted in the wide-spread availability of cost-effective technology to collect, transmit, store, analyze and use information in electronic formats. As a result, entities now have the ability to readily collect and analyze vast amounts of information. This has created tensions between: (a) the increasing quantity of information available to qualify prospects, develop personalized / customized offerings for potential customers and / or conduct health-related or other research; and (b) decreasing security, anonymity and privacy for individuals who often are not aware of the existence of many data elements that may be traced back to them, and over which they often have little or no effective control.

[0006] Data elements may be collected both online and offline (both "born digital" and "born analog" and converted into digital format at a later date) through a variety of sources including, but not limited to, activity on social networking sites, electronic or digital records, emails, participation in rewards or bonus card programs that track purchases and locations, browsing or other activity on the Internet, and activity and purchases at brick-and-mortar stores and / or on e-commerce websites. Merchants, medical-related and other service providers, governments, and other entities use this tremendous amount of data that is collected, stored, and analyzed to suggest or find patterns and correlations and to draw useful conclusions. This data is sometimes referred to as "big data," due to the extensive amount of information entities may now gather. With big data analytics, entities may now unlock and maximize the value of data - one example may involve non-health related entities engaging in behavioral marketing (with materials created for distribution being customized in an attempt to increase the correlation with the preferences pertaining to a particular recipient party) and another example may involve heath-related entities accessing big data to conduct medical research. However, with behavioral marketing and big data analytics, related parties now have a much lower level of privacy and anonymity.

[0007] Attempts at reconciling the conflict between privacy / anonymity and value / personalization / research have often historically involved using alternative identifiers rather than real names or identifying information. However, these alternative identifiers are generally statically assigned and persist over time. Static identifiers are more easily tracked, identified, and cross-referenced to ascertain true identities, and may be used to ascertain additional data about subjects associated with data elements without the consent of related parties. Privacy and information experts have expressed concerns that re-identification techniques may be used with data associated with static identifiers and question whether data that is identifiable with specific computers, devices or activities (i.e., through associated static identifiers) can in practice be considered anonymous or maintained in a protected state of anonymity. When an identifier does not change over time, adversarial entities have unlimited time to accrete, analyze and associate additional or even exogenous data with the persistent identifier, and thus to determine the true identity of the subject and associate other data with the true identity. In addition, unlimited time provides adversarial entities with the opportunity to perform time-consuming brute-force attacks that can be used against any encrypted data.

[0008] According to a 2011 McKinsey Global Institute report:

- A retailer using big data to the full extent could increase its operating margin by more than 60 percent;
- Harnessing big data in the public sector has enormous potential - if U.S. healthcare were to use big data creatively and effectively to drive efficiency and quality, the sector could create more than $300 billion in value every year - two-thirds of that would be in the form of reducing US healthcare expenditure by about 8 percent;
- In the developed economies of Europe, government administrators could save more than €100 billion ($149 billion) in operational efficiency improvements from using big data, not including using big data to reduce fraud and errors and boost the collection of tax revenues; and
- Users of services enabled by personal-location enabled big data could capture $600 billion in consumer surplus.

[0009] Many potential benefits from big data have not been fully realized due to ambiguity regarding ownership / usage rights of underlying data, tensions regarding privacy of underlying data, and consequences of inaccurate analysis due to erroneous data collected from secondary (versus primary) sources and / or inferred from activities of parties without active participation of, or verification by, said parties.

[0010] What are needed are systems, methods and devices that overcome the limitations of static and / or persistent privacy / anonymity and security systems and improve the accuracy of data for exchange, collection, transactions, analysis and other uses-especially in identity-sensitive and / or context-sensitive applications. Put another way, privacy / anonymity-enhancing technologies, such as those described herein, can help to reconcile the tensions between identifiable and functional information by providing tools that enable trust and control in order to achieve the privacy / anonymity goals of both individuals and users of such information.

[0011] US 2011/0010563 A1 discloses a method and apparatus for anonymous data processing. The appended claims are characterised over this document.

Summary

[0012] The present invention relates to a system as claimed in claim 1, a corresponding non-transitory computer readable medium as claimed in claim 9 and a method as claimed in claim 13. Preferrred embodiments are defined in the dependent claims. Embodiments of the present invention may improve data privacy 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. Embodiments of the present invention may include systems, methods and devices that create, access, use (e.g., collecting, processing, copying, analyzing, combining, modifying or disseminating, etc.), store and / or erase data with increased privacy, anonymity and security, thereby facilitating availability of more qualified and accurate information. And, when data is authorized to be shared with third parties, embodiments of the present invention may facilitate sharing information in a dynamically controlled manner that enables delivery of temporally-, geographically-, and / or purpose-limited information to the receiving party.

[0013] As compared to existing systems, wherein electronic data may be readily accessible for use (e.g., collecting, processing, copying, analyzing, combining, modifying or disseminating, etc.), storing and / or erasing with few effective controls over the data, embodiments of the present invention may use temporally unique, dynamically changing de-identifiers ("DDIDs")- each associated with a subject, e.g., a person, place, or thing, to which data directly or indirectly pertains or relates (a "Data Subject"), and / or an action, activity, process and / or trait pertaining to a Data Subject, for a temporally unique period of time, thereby enabling the Data Subject to operate in a "dynamically anonymous" manner. "Dynamically anonymous" or "Dynamic Anonymity" as used herein, refers to a user's ability to remain anonymous until such time as a decision is made not to remain anonymous, at which time only the desired information is shared with one or more desired parties in connection with one or more actions, activities, processes or traits. Embodiments of the present invention may thereby enable the ability of Data Subjects to maintain flexible levels of privacy and / or anonymity under the control of a Data Subject or controlling entity that may be a trusted party or proxy.

[0014] Embodiments of the invention may use DDIDs to help prevent the retention of data, sometimes referred to as metadata, that may otherwise provide third parties with information about one or more aspects of a Data Subject and / or data attributes reflecting actions, activities, processes and / or traits pertaining to a Data Subject, such as, by way of example and not limitation, information pertaining to means of creation, purpose, time and / or date of creation, identity of the Data Subject and / or creator of the data attributes, location where data attributes were created, standards used in creating or using data attributes, etc. This is due to the fact that metadata must have something to attach itself to - or to associate itself with - in order to establish an ongoing record of information associated with one or more specific data attributes. The words "data," "attributes," "elements" or similar terms used in this application will include, any or all of the following, as applicable, (i) structured data (i.e., data in predetermined structured schemas), (ii) unstructured data, (iii) metadata (i.e., data about data), (iv) other data, and / or (v) any of the foregoing types of data initially recorded in analog format and later converted into digital format.

[0015] Embodiments of the present invention may use a first DDID at one time for a specific purpose pertaining to a first Data Subject, action, activity, process and / or trait, and then use a second DDID in association with the first Data

Subject, action, activity, process and / or trait, for a different purpose, and / or use the first DDID in association with a second Data Subject, action, activity, process and / or trait, for a different purpose, etc. As a result, attempts to retain and aggregate data associated with underlying information associated with DDIDs may be ineffective since different DDIDs may be associated with the same Data Subject, action, activity, process and / or trait, and / or the same DDID may be used with different Data Subjects, actions, activities, processes and / or traits, and / or purposes - each for a temporally unique period of time.

[0016] Embodiments of the present invention may track and record different DDIDs used by, and associated with, Data Subjects at different times with respect to various actions, activities, processes or traits thereby enabling the storage, selection and retrieval of information applicable to a specific action, activity, process or trait and / or a specific Data Subject. Conversely, the system may not enable third parties external to the system to effectively retain and aggregate data due to the use of multiple DDIDs and the lack of information available external to the system to determine relationships between and among DDIDs and / or Data Subjects, actions, activities, processes and / or traits.

[0017] Each DDID may be associated with any one or more data attributes to facilitate with respect to a specific action, activity, process or trait, such as, by way of example and not limitation: (a) information reflecting an action, activity, process or trait associated with a Data Subject while associated with a current DDID (e.g., browsing information reflecting current web-based activity of a Data Subject while being associated with a current DDID) before the current DDID is replaced with a different DDID; (b) information with respect to past actions, activities, processes or traits previously associated with a Data Subject while associated with one or more previous DDIDs but with respect to which the Data Subject now desires to share information with a third party while associated with the current DDID (e.g., sharing pricing information with an e-commerce website that the Data Subject collected from said website in a previous browsing session while being associated with a previous DDID); and (c) new information that may help facilitate with respect to a desired action, activity, process or trait on behalf of the Data Subject while associated with a current DDID (e.g., indicating new desired size and color for a currently desired purchase of clothing from an e-commerce website). For purposes hereof, the combination of a DDID and any data elements associated with the DDID for a temporally unique period of time are referred to as a temporal data representation, or a "TDR." For purposes hereof, if no data is associated with a DDID, then a DDID and its temporal data representation (or "TDR") are identical.

[0018] From the perspective of an implementation of an embodiment of Dynamic Anonymity being a closed system, a DDID intended to represent the identity of a Data Subject, i.e., a "primary identifier," is required to be temporally unique during the time period of the assignment of the DDID to the Data Subject - i.e., no two extant Data Subjects can have identical primary identifier DDIDs at the same time. The requirement for temporal uniqueness of DDIDs is applicable when separateness of identity of Data Subjects is desired to be represented by DDIDs; if factors other than separateness of identity of Data Subjects are desired to be represented by DDIDs, DDID assignments can be made accordingly to represent intended associations, relationships, etc. DDIDs can be instantiated in two ways: (i) within an implementation of the present invention or (ii) by externally created identifiers, but only provided that they satisfy the "temporally unique" requirement (e.g., a "cookie" or other unique identifier assigned by a website to a first-time visitor could effectively serve as a DDID) when separateness of identity of Data Subjects is desired to be represented by DDIDs.

[0019] A cookie is a small piece of data that is generally sent from a website and stored in a Data Subject's web browser while the Data Subject is browsing the website, so that, every time the Data Subject returns to the website, the browser sends the cookie back to a server associated with the website to notify the website the Data Subject has returned to the website. However, in order for a cookie to serve as a DDID, the browser (serving as the client in this potential embodiment of the invention) may prevent any cookie submitted by the website from persisting between browsing sessions (e.g., by copying the user's cookies, cache and browsing history files to the anonymity system's servers and then deleting them off the user's computer), such that a new cookie may be assigned for each browsing session. In this manner, the various cookies (in this example embodiment, serving as DDIDs representing separateness of identity of Data Subjects) issued by the website, while being created "externally" to the system, would each be unique and would not enable the website to remember stateful information or aggregate the Data Subject's browsing activity, since each of the browsing sessions would be perceived by the website as unrelated-thereby enabling the Data Subject to remain dynamically anonymous as long as desired, to the extent desired.

[0020] As mentioned in the example potential embodiment above, the Dynamic Anonymity system, according to some embodiments, may collect and retain information related to the various actions, activities, processes or traits associated with the different browsing sessions / different cookies (in this example, serving as DDIDs representing separateness of identity of Data Subjects) and store the combined information in an aggregated data profile for the Data Subject until such time as a decision is made by, or on behalf of, the Data Subject to no longer remain anonymous, at which point only desired information from the Data Subject's aggregated data profile need be shared with one or more desired parties in connection with one or more actions, activities, processes or traits. In this exemplary embodiment of the invention, this may involve the Data Subject deciding to provide information to a website from the Data Subject's aggregated data profile as a TDR that reflects past activity of the Data Subject on the website-all at the election and control of the Data Subject (or other controlling entity). In the above exemplary embodiment of the invention, in lieu of using cookies assigned

by a website visited by a Data Subject as DDIDs, the system may alternatively use globally unique identifiers (GUIDs) (i.e., unique reference numbers used as identifiers in computer software), or other temporally unique, dynamically changing proxy de-identifiers, as DDIDs whether created internally by, or externally to, implementations of the present invention. In the above examples, control over the collection of data resulting from browsing activity by a Data Subject would reside with the Data Subject or other controlling entity, rather than with the websites visited by the Data Subject. In still other exemplary embodiments of the invention, rather than the Data Subject deciding when to send, i.e., "push," information to the website from the Data Subject's aggregated data profile, a website (with proper permissions and authentication) could request, i.e., "pull" the relevant information and / or relevant DDID-to-Data Subject association information from the Data Subject's aggregated data profile at such time that the information is needed by the website.

[0021] In still other exemplary embodiments of the invention, the work to dynamically anonymize and control the sending of the relevant portions of the Data Subject's aggregated data profile may be handled by: the Data Subject's client device itself; the central Dynamic Anonymity system referred to above; or a combination of the two. For example, a complete view of a particular Data Subject's information and / or relevant DDID-to-Data Subject association information for a predetermined or flexible amount of time could be stored at the Data Subject's client device for the predetermined or flexible amount of time, before then being synchronized back to a central Dynamic Anonymity system (as well as synchronized with any other client devices that the Data Subject may have registered with the central anonymity system).

[0022] TDRs and DDIDs may comprise multiple levels of abstraction for tracking and identification purposes. A system according to some embodiments of the present invention may store the TDRs (consisting of DDID values and data elements, if any, associated with the DDIDs), as well as information regarding the time period during which each DDID was associated with a particular Data Subject, data attribute(s), action, activity, process or trait-thereby allowing the TDRs to be re-associated at a later time with the particular Data Subject, data attribute(s), action, activity, process or trait. Such a system may be utilized to facilitate the development of aggregated data profiles by reference to and with the use of keys that reveal the relationship between and among various DDIDs, Data Subjects, data attributes(s), actions, activities, processes and / or traits. In other words, "Dynamic Anonymity," as afforded by the use of TDRs and / or DDIDs, as described herein, may enable Data Subjects to benefit from ongoing technological advancements (e.g., the Internet of Things (IoT), personalized medicine, etc.) without having to relinquish privacy, anonymity, security or control. This may be accomplished by: (i) assigning unique dynamically changing DDIDs to Data Subjects, actions, activities, processes and / or traits; (ii) retaining information regarding association of DDIDs with Data Subjects, actions, activities, processes and / or traits; and (iii) providing Data Subjects and / or controlling entities, that may be trusted parties / proxies, with deterministic control over access to / use of association information. With the use of dynamically changeable, temporally unique, and re-assignable DDIDs, current systems and processes (e.g., web browsers and data analytic engines) may not be able to recognize relationships between and among disassociated and / or replaced data elements. They may still process information using existing capabilities, but will do so without creating inferences, correlations, profiles or conclusions-except as expressly authorized by Data Subjects and trusted parties / proxies. Moreover, the DDIDs employed by embodiments of the present invention can be replaced dynamically at the data element-level enabling Dynamic Anonymity - not just at the Data Subject-level or data record-level. This means that individuals may have control over what data is shared or accessed, enabling dynamic de-identification without "de-valuation" of the underlying information.

[0023] Control of information down to the data element-level makes controlled information sharing possible in the age of big data-beyond the reach of controls targeted only at the data record-level or Data Subject-level. It further enables a "one and done relationship" between a Data Subject and a website or other entity receiving information about the Data Subject. Most existing systems collect information around a unique identifier over time. Even if a DDID carries with it a certain amount of history or other information pertaining to a Data Subject, the next time the Data Subject visits the site, store, doctor, etc. the Data Subject could look like a completely different Data Subject if desired. Only when and if the DDID contained a unique identifier, a name or email address for example, could a recipient correlate a then-current DDID representing the Data Subject with a DDID previously used to represent the Data Subject, at which point the recipient could interact with the Data Subject based on the recipient's collection of data on the Data Subject. However, the next time the recipient encounters the Data Subject, the Data Subject would not be re-identifiable unless desired by the Data Subject.

[0024] Dynamic Anonymity also enables controlled "data fusion" (wherein "data fusion" is defined as being what occurs when data from different sources are brought into contact with each other and new facts emerge) by providing controlled anonymity for data, identity (of the Data Subject and / or the controlling entity) and context (e.g., time, purpose, place) by obfuscating connections between and among the foregoing. Dynamic Anonymity thus also enables the undoing or reversal of either rights granted or access to data (e.g., a particular party could be provided with access to data underlying a DDID then have their access revoked via the changing of Replacement Keys), as well as the rejuvenation of data (i.e., of the values of the data, not necessarily re-identification) of data to support additional authorized secondary uses without violating promises to Data Subjects (e.g., one or more DDIDs may initially provide access via one or more Replacement Keys to the results of an X-ray and, via the changing of Replacement Keys, later reflect the results of the X-ray as well

as results of follow-on physical therapy).

[0025] The reason Dynamic Anonymity will still be attractive in the commercial marketplace is that companies often do not actually care *who* the Data Subjects they interact with are (i.e., their actual, "real world" identities); they instead care *what* the Data Subjects are; *how* the Data Subjects behave; and *when* the Data Subjects behave that way. The more accurate their targeting is and the less wasteful, the more likely an anonymous consumer will respond favorably to a personalized offering. Dynamic Anonymity thus obviates the need for companies to follow Data Subjects around the digital world to try to persuade them to buy products and / or services that they may not really need or want. Dynamic Anonymity allows for more profitable "matching" of sellers and interested customers. Currently, the best that many companies can do is to "segment" potential customers by using demographics and statistics, but they may have no idea of the actual interest of individual segment members. Dynamic Anonymity also improves upon generalized demographics and statistics by providing individualized expressions / levels of expression of interest from members of segments who are "highly qualified" prospects. The ability of Dynamic Anonymity to enable Data Subjects to directly or indirectly control use of their data in accordance with their personal privacy / anonymity preferences can support disparate treatment of data in disparate jurisdictions notwithstanding different data use / privacy / anonymity requirements in such jurisdictions (e.g., differences between European Union "fundamental right" and U.S. balancing of privacy rights / right to free expression / commerce perspectives on data privacy / anonymity protection).

[0026] In the context of healthcare, medical-related and other areas of research, Dynamic Anonymity will be more attractive than traditional approaches to "de-identification" that protect data privacy / anonymity by using a defensive approach - e.g., a series of masking steps are applied to direct identifiers (e.g., name, address) and masking and / or statistically-based manipulations are applied to quasi-identifiers (e.g., age, sex, profession) in order to reduce the likelihood of re-identification by unauthorized third parties. This defensive approach to protecting data privacy / anonymity results in a tradeoff between protecting against re-identification and retaining access to usable information. In comparison, with Dynamic Anonymity the value of information can be retained and leveraged / exploited for authorized purposes, all with a statistically insignificant risk of re-identification of any datum. DDIDs can be used to represent actions, activities, processes and / or traits between and among Data Subjects, the meaning of which may change over time thereby requiring the then-current appropriate key(s) to discern underlying values. Dynamic Anonymity therefore rejects the proposition and traditional dichotomy that, in order to minimize the risk of / anonymity loss, one must sacrifice information content by making it forever unrecoverable. Instead, Dynamic Anonymity minimizes both the risk of privacy / anonymity loss and the amount of information lost, enabling most - if not all - of it recoverable, but only with authorization.

[0027] Keys used by embodiments of the present invention may vary depending on the use of corresponding DDIDs. For example: time keys ("TKs") may be used to correlate the time period of association between a DDID and a Data Subject, action, activity, process and / or trait - i.e., the time period of existence of a TDR; association keys ("AKs") may be used to reveal the association between two or more data elements and / or TDRs that may not otherwise be discernibly associated one with another due to the use of different DDIDs; replacement keys ("RKs") may be used if / when DDIDs are used in replacement of one or more data attributes within a TDR, in which case look-up tables may be referenced to determine the value of the one or more data attributes replaced by the said one or more DDIDs included within the TDR.

[0028] Without access to the applicable TK(s), AK(s) and / or RK(s), in the event that a third party intercepts information pertaining to one or more Data Subjects, actions, activities, processes and / or traits, the third party would not be able to: (i) re-identify a Data Subject by means of associating DDIDs and corresponding data attributes (which together comprise TDRs) in the case of the association function of the present invention; and / or (ii) knowing the value of data elements represented by DDIDs so as to correctly understand the information in the case of the replacement function of the present invention. Conversely, embodiments of the present invention may enable a Data Subject or other controlling entity to send to one or more desired third parties only those data attributes (which the system knows relate to the Data Subject by virtue of the tracking / logging / recording functions of the system) that specifically pertain to a specific action, activity, process or trait.

[0029] Disclosed herein are various systems, methods and devices for private and secure management and use of information pertaining to one or more Data Subjects, such as persons, places or things, and associated actions, activities, processes and / or traits. The systems, methods and devices described herein may abstract data pertaining to Data Subjects, actions, activities, processes and / or traits by linking elements pertaining to the data into independent attributes or dependent attributes, separating elements pertaining to the data into independent attributes or dependent attributes. For purposes of this disclosure, an attribute refers to any data element that can be used, independently or in combination with other data elements, to directly or indirectly identify a Data Subject, such as a person, place or thing, and associated actions, activities, processes and / or traits. It should be noted that a Data Subject may have attributes or attribute combinations that are unique to the Data Subject: for example, an individual Data Subject's social security number, as well as attributes or attribute combinations that are shared by the Data Subject with other Data Subjects: for example, an individual Data Subject's sex or affiliation with a political party. In some instances, an attribute may be an electronic or digital representation of a Data Subject or associated action, activity, process and / or trait. Similarly, attributes may be electronic or digital representations of information or data related to a Data Subject or associated action, activity,

process and / or trait. Separating, linking, combining, rearranging, defining, initializing or augmenting the attributes, can form attribute combinations pertaining to any particular Data Subject or group of Data Subjects, or associated actions, activities, processes and / or traits. With respect to any Data Subject, action, activity, process and / or trait, the attribute combinations may include any combination of attributes, as well as other data that is added to or combined with the attributes. It should be further noted that an attribute or combination of data attributes may identify a Data Subject but are not themselves the Data Subject - the person or legal entity identified by an attribute or combination of data attributes may be the subject of said attribute or combination of data attributes and considered a related party with regard thereto since he / she / it has an interest in or association with said attribute or combination of data attributes. In addition, parties (other than a Data Subject identified by an attribute or combination of data attributes) who have an interest in or association with an attribute or combination of data attributes may also be considered related parties with regard to the attribute or combination of data attributes.

[0030] In some embodiments, a client-server structure or architecture may be utilized to implement one or more features or aspects of this disclosure, whether on premises in or across an enterprise, in a private or public cloud, in a private or public hybrid cloud, or in any combination of the foregoing, whereby in one example, a privacy server, which may be virtual, logical or physical, provides functions and / or services to one or more privacy clients, which themselves may be virtual, logical or physical. These privacy clients that may reside on a Data Subject device, on a service provider device, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server may initiate requests for such functions and / or services by interacting with data attributes and / or data attribute-to-Data Subject association information stored in a database on a hard drive or other memory element associated with the privacy server. For example, a data attribute may be linked to independent attributes or dependent attributes or separated into independent attributes or dependent attributes by means of a privacy server coupled to the database in response to requests for functions and / or services from one or more privacy clients. It should be noted that implementations of the invention may use a single computer or computing device as both a privacy server and a privacy client whereas other implementations may use one or more computers or computing devices located in one or more locations as a privacy server and one or more computers or computing devices located in one or more locations as a privacy client. A plurality of system modules may be used to perform one or more of the features, functions and processes described herein, such as but not limited to: determining and modifying required attributes for attribute combinations; assigning DDIDs; tracking DDID use; expiring or re-assigning existing DDIDs; and enabling or providing data associations relevant to or necessary with respect to a given action, activity, process or trait.

[0031] In one embodiment, these modules may include an abstraction module of the privacy server configured to among other things: dynamically associate at least one attribute with at least one Data Subject, action, activity, process and / or trait; determine and modify required attributes relevant to or necessary for a given action, activity, process or trait; generate, store, and / or assign DDIDs to the at least one data attribute to form a TDR; and assign a predetermined expiration to a TDR by means of the DDID component of the TDR.

[0032] These system modules, and if desired other modules disclosed herein, may be implemented in program code executed by a processor in the privacy server computer, or in another computer in communication with the privacy server computer. The program code may be stored on a computer readable medium, accessible by the processor. The computer readable medium may be volatile or non-volatile, and may be removable or non-removable. The computer readable medium may be, but is not limited to, RAM, ROM, solid state memory technology, Erasable Programmable ROM ("EPROM"), Electrically Erasable Programmable ROM ("EEPROM"), CD-ROM, DVD, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic or optical storage devices. In certain embodiments, privacy clients may reside in or be implemented using "smart" devices (e.g., wearable, movable or immovable electronic devices, generally connected to other devices or networks via different protocols such as Bluetooth, NFC, WiFi, 3G, etc., that can operate to some extent interactively and autonomously), smartphones, tablets, notebooks and desktop computers, and privacy clients may communicate with one or more privacy servers that process and respond to requests for information from the privacy clients, such as requests regarding data attributes, attribute combinations and / or data attribute-to-Data Subject associations.

[0033] In one implementation of the present invention, DDIDs associated with attributes and attribute combinations may be limited in scope and duration. Further, DDIDs may be re-assignable, such that a DDID may refer to multiple Data Subjects or multiple actions, activities, processes or traits at different points in time. The DDIDs may be re-assignable on a configurable basis in order to further abstract and dilute or attenuate data trails while maintaining the timeliness and saliency of the TDRs and data contained therein.

[0034] In one example, rather than storing, transmitting or processing all data attributes pertaining to a Data Subject and / or relevant to or necessary for a given action, activity, process, or trait, embodiments of the present invention may introduce an initial layer of abstraction by means of an association function, e.g., by including only a portion of the relevant data attributes in each TDR. In this way, the data attributes pertaining to a Data Subject may be disassociated within seemingly unrelated TDRs, such that access to and use of one or more AKs are necessary in order to know which two or more TDRs must be associated with each other in order to collectively contain all the data attributes pertaining to a

Data Subject and / or that are relevant to or necessary for a given action, activity, process or trait. The privacy, anonymity and security of data attributes contained or referenced within a TDR may be further improved or enhanced by means of a replacement function, e.g., by replacing one or more of said data attributes contained in one or more TDRs with DDIDs so that access to and use of one or more RKs are necessary to enable use of look-up tables to determine the value of the one or more data elements replaced by said one or more DDIDs. The privacy, anonymity and security of data attributes contained or referenced within a TDR may be further improved or enhanced by using other known protection techniques, such as encrypting, tokenizing, pseudonymizing, eliding and / or otherwise; and / or by introducing additional layers of abstraction by replacing keys with second-level or n-level DDIDs.

[0035] In the case of both: disassociation of data attributes pertaining to a Data Subject, action, activity, process and / or trait, so as to require AKs; and replacement of data attributes pertaining to a Data Subject, action, activity, process and / or trait, so as to require RKs, the effective level of privacy, anonymity and security may be enhanced based on how, and how often, the DDIDs associated with the data attribute or attributes in question are changed and / or are changeable. In one exemplary embodiment of the invention, DDIDs may be assigned for purposes of disassociation and / or replacement and retain their initially assigned value(s) - i.e., permanent assignments. In another exemplary embodiment of the invention, DDIDs may be assigned for purposes of disassociation and / or replacement and retain their initially assigned value(s) until the value(s) are changed on an ad hoc basis, i.e., "ad hoc changeability." In yet another exemplary embodiment of the invention, DDIDs may be assigned for purposes of disassociation and / or replacement and retain their initially assigned value(s) until the value(s) are changed based on a random, fixed, variable or other dynamic basis, i.e., "dynamic changeability."

[0036] Embodiments of the present invention may create additional layers of abstraction by replacing identifying references within the system to external networks, internets, intranets, and / or computing devices that may be integrated, or communicate, with one or more embodiments of the present invention with DDIDs so that one or more RKs and / or AKs are necessary to enable access to and use of look-up tables to determine the identity of the one or more external networks, internets, intranets, and / or computing devices replaced by said one or more DDIDs.

[0037] Due to the changeable, temporally unique, and re-assignable characteristics of DDIDs paired with data attributes or attribute combinations to create TDRs, recipients of TDRs may make use of information contained in TDRs specifically for intended purposes at intended times. This is due to the fact that Association Keys (which may be required to stitch TDRs together to make sense of information contained in seemingly unrelated TDRs) and / or Replacement Keys (which may be required to know the value of information represented by temporally unique DDIDs sent to third parties as part of TDRs) may only have temporally limited usefulness. In other words, the usefulness is temporally limited because the DDID components of TDRs may be changed by a Data Subject or other controlling party when the intended purpose and / or intended time is no longer applicable in such a manner that AKs and / or RKs no longer reveal relevant information. Conversely, relevant information revealed by means of AKs and / or RKs may change over time to support additional secondary uses of data.

[0038] In one example, a maintenance module may be utilized to store information regarding the association at any particular point in time of a particular DDID with a particular attribute combination in a TDR in a secure database associated with the privacy server and accessible by the system but not accessible by parties other than the controlling entity or by parties authorized by the controlling entity (this time period of association may be represented by a time key (TK) or otherwise). In one example, the maintenance module of the privacy server and associated database(s) may store and keep all associations of DDIDs with attribute combinations. Thus, the system provides for secure data exchange and non-repudiation of data attributes, attribute combinations and TDRs in order to foster safer data-related collection, use, research and / or analysis while meeting stringent privacy, anonymity and security criteria.

[0039] In one example, a verification module of the privacy server and associated database(s) may provide an authenticated data structure that permits validation and verification of the integrity of information and / or DDIDs embodied in an aggregated data profile, data attributes, attribute combinations and / or TDRs at any point in time through methodologies such as cyclic redundancy checks ("CRCs"), message authentication codes, digital watermarking, linking-based time-stamping or analogous methodologies.

[0040] In another example, an authentication module of an embodiment of the present invention may be used to verify, on an anonymous basis, the authority to proceed with respect to a Data Subject, action, activity, process or trait at a particular time and / or place via the TDR assignment. A privacy client with TDR information may request of the authentication module, which in one example is part of the privacy server, confirmation as to whether the TDR (and undisclosed Data Subject, data attributes or attribute combinations associated therewith) is authorized to participate with regard to a requested action, activity, process or trait at a particular time and / or place. In one embodiment, the authentication module may compare the DDID included in the TDR to a list of authorized DDIDs to determine the state of authorization to participate with respect to a desired action, activity, process or trait at the specified time and / or place. Optionally, the authentication module may request the party possessing the TDR to confirm it is authorized to participate with respect to a desired action, activity, process or trait at the specified time and / or place through DDID confirmation or other confirmation techniques such as password confirmation or multi-factor authentication. If an optional authorization request

is made, the process continues only if the party is authorized, in one example. The authentication module may transmit the authorization status information to the party controlling the TDR via a privacy client, and the authorization status may be used to allow or deny proceeding with respect to a desired action, activity, process or trait at the specified time and / or place.

[0041] TDRs and / or DDIDs contained in TDRs can also be used as advanced keys for known protection techniques such as encrypting, tokenizing, pseudonymizing, eliding or otherwise. The authentication module may be used to withhold the key necessary to unlock protection techniques for the contents of the TDR such as encrypting, tokenizing, pseudonymizing, eliding or otherwise, unless the TDR, DDID, undisclosed associated Data Subject, attribute, attribute combination or related party is confirmed as being authorized to participate with respect to a desired action, activity, process or trait at the specified time and / or place through DDID and / or TDR confirmation and known confirmation techniques such as password confirmation, multi-factor authentication or similar means.

[0042] In another example, an access log module may be provided, wherein the access log module can collect and store information to enable post-incident forensic analysis in the event of a system or privacy server error and / or misuse.

[0043] In accordance with one aspect of one embodiment of the present invention, disclosed herein is a computer-implemented method of providing controlled distribution of electronic information. In one example, the method may include the steps or operations of receiving, at a computing device, data; identifying one or more attributes of the data; selecting, through the computing device, a DDID; associating the selected DDID with one or more of the data attributes; and creating a temporally unique data representation (TDR) from at least the selected DDID and the one or more data attributes.

[0044] In one example, the step of selecting a DDID may include generating the temporally unique, dynamically changing DDID or, in another example, accepting or modifying a temporally unique, dynamically changing value created external to the system to serve as the DDID.

[0045] For purposes hereof, the phrase "dynamically changing" means that a DDID assigned with respect to a data subject, action, activity, process or trait: (a) changes over time due to (i) passage of a predetermined amount of time, (ii) passage of a flexible amount of time, (iii) expiration of the purpose for which the DDID was created, or (iv) change in virtual or real-world location associated with the data subject, action, activity, process or trait; or (b) is different at different times (i.e., the same DDID is not used at different times) with respect to a same or similar data subject, action, activity, process or trait.

[0046] For purposes hereof, the phrase "temporally unique" means that the time period of assignment of a DDID to a data subject, action, activity, process or trait is not endless. The initial assignment of a DDID to a data subject, action, activity, process or trait starts at a point in time, and information concerning the time of assignment is known and, in certain implementations of the present invention, may be used to identify relationships or connections between the DDID and said data subject, action, activity, process or trait. If the period of assignment of a DDID to a data subject, action, activity, process or trait ends at a discrete point in time, information concerning the time of termination of assignment is known and, in certain implementations of the present invention, may be used to identify relationships or connections between the DDID and said data subject, action, activity, process or trait.

[0047] In another example, the method may also include causing the association between the selected DDID and the one or more data attributes to expire. In yet another example, the method may include storing, in a database accessible to the computing device, information regarding the time periods during which the selected DDID was associated with different data attributes or combinations of attributes by means of time keys (TKs) or otherwise.

[0048] In another embodiment, the method may also include re-associating the selected DDID with one or more other data attributes or attribute combinations following expiration of the association between the DDID and one or more initial data attributes.

[0049] In one example, the expiration of the DDID occurs at a predetermined time, or the expiration may occur following completion of a predetermined event, purpose or activity. In another example, the DDID may be authorized for use only during a given time period and / or at a predetermined location.

[0050] In another example, the method may include changing the DDID associated with the one or more data attribute, attribute combination and / or TDR, wherein the changing the DDID may occur on a random or a scheduled basis, or may occur following the completion of a predetermined activity purpose and / or event.

[0051] According to another aspect of another embodiment of the present invention, disclosed herein is a method for facilitating transactions over a network, wherein the method may include the operations of receiving a request, at a privacy server, from a client device to conduct activity over a network; determining which of a plurality of data attributes or attribute combinations in a database is necessary to complete the requested activity; creating or accepting a DDID; associating the DDID with the determined data attributes to create a combined temporally unique data representation (TDR); making the combined temporally unique data representation (TDR) accessible to at least one network device for conducting or initiating the requesting activity; receiving a modified temporally unique data representation (TDR) that includes additional information related to the activity performed; and storing the modified temporally unique data representation (TDR) and / or DDID-to-Data Subject association information in a memory database.

[0052] In one example, the at least one network device may include an internet service provider, a server operated by a merchant or service provider, a server operated by a mobile platform provider, or a server in a cloud computing environment.

[0053] According to another aspect of another embodiment of the present invention, disclosed herein is a method of providing controlled distribution of electronic information. In one example, the method may include receiving a request at a privacy server to conduct an activity over a network; selecting attributes of data located in a database accessible to the privacy server determined to be necessary to fulfill the request, wherein other attributes of the data which are not determined to be necessary are not selected; assigning or accepting the assignment of a DDID to the selected attributes, and / or attribute combinations to which they apply with an abstraction module of the privacy server, wherein the DDID does not reveal the unselected attributes; recording the time at which the DDID is assigned; receiving an indication that the requested activity is complete; receiving the DDID and the determined attributes and / or attribute combinations to which they apply at the privacy server, wherein the attributes are modified to include information regarding the conducted activity; and recording the time at which the conducted activity is complete and the DDID and the determined attributes and / or attribute combinations to which they apply are received at the privacy server.

[0054] In one example, the method may also include assigning an additional DDID to one or more of the selected data attributes and / or attribute combinations contained within a TDR. In another example, the method may include re-associating, using time keys (TKs) reflecting recorded times, the DDID and data attributes with the true identity of the data attributes, attribute combinations, or Data Subjects. The method may also include reassigning the DDID to other data attributes, and recording the time at which the DDID is reassigned.

[0055] According to another aspect of another embodiment of the present invention, disclosed herein is a computer-implemented method of improving data security, wherein the data comprises at least one attribute. In one example, the method may include associating at least one attribute with a DDID to create a temporally unique data representation (TDR); wherein the temporally unique data representation (TDR) limits access to data attributes to only those necessary to perform a given action, such as for example completing a purchase of goods from an online website.

[0056] In one example, the method may include assigning an association key (AK) to the temporally unique data representation (TDR), wherein access to the association key (AK) is required for authorized access to the temporally unique data representation (TDR).

[0057] In another example, the method may also include causing the association between the DDID and the at least one attribute to expire, wherein the expiration occurs at a predetermined time and / or the expiration may occur following completion of a predetermined event and / or activity. In another embodiment, the method may include re-associating the DDID with the at least one different attribute following an expiration of the association between the DDID and the at least one attribute. The method may also include storing, in a database, information regarding one or more time periods during which the DDID was associated with different data attributes or combinations of attributes as reflected by applicable time keys (TKs) or otherwise.

[0058] According to another aspect of another embodiment of the present invention, disclosed herein is a system for improving electronic data security. In one example, the system may include a module configured to dynamically associate at least one attribute with at least one Data Subject, action, activity, process and / or trait; a module configured to generate or accept DDIDs, and further configured to associate DDIDs to the at least one data attribute; a module configured to track activity related to the DDIDs, and configured to associate any additional electronic data generated by the activity to the DDID; and a module for storing the DDIDs, tracked activity, and time periods during which a DDID is used for conducting the tracked activity.

[0059] According to another aspect of another embodiment of the present invention, disclosed herein is a device for conducting secure, private activity over a network. In one example, the device may include a processor configured to execute program modules, wherein the program modules include at least a privacy client; a memory connected to the processor; and a communication interface for receiving data over a network; wherein the privacy client is configured to receive temporally unique data representations (TDRs) including DDIDs and associated data attributes necessary for conducting the activity over the network from a privacy server.

[0060] In one example, the privacy client may be further configured to capture activity conducted using the device, and to relate the conducted activity to the temporally unique data representations (TDRs). In another example, the privacy client may be configured to transmit the captured activity and temporally unique data representations (TDRs) to the privacy server. The privacy client may reside on a mobile device as a mobile application, in one example. The privacy client may reside in, and be accessible via, a network as a cloud based application, in another example. The privacy client may reside on the same computing device(s) on which the privacy server(s) resides as a local application, in another example.

[0061] In another example, the device may also include a geolocation module on a mobile device, wherein the temporally unique data representations (TDRs) are modified with information from the geolocation module, and wherein the temporally unique data representations (TDRs) restrict access to information regarding the identity of the device. The device may also include a user interface configured to allow a user to modify the temporally unique data representations

(TDRs), including options to change the DDID or data attributes associated with a particular temporally unique data representation (TDR). The user interface may include selectable options for sharing the temporally unique data representations (TDR) only with other network devices within a predetermined physical, virtual or logical proximity to the mobile device.

[0062] In another example, the device may, in response to the shared temporally unique representations (TDRs), receive targeted advertising or marketing information based on the physical, virtual, or logical location of the mobile device, wherein the shared temporally unique data representations (TDRs) may in one example include demographic information, temporal information, geolocation information, psychographic information and / or other forms of information related to a user of the mobile device. In another example, the shared temporally unique data representations (TDRs) may include information related to purchase transactions made or desired to be made using the mobile device, and further comprising receiving targeted advertising or marketing information based on previous or desired purchase transactions. In this way, a vendor may nearly instantly know the relevant characteristics of nearby users and potential customers-without knowing or learning the identity of such users-so that the vendor may tailor product and service offerings specifically to the interests of nearby users and potential customers in real-time without compromising the privacy / anonymity of the users / potential customers.

[0063] According to another aspect of another embodiment of the present invention, disclosed herein is a system for providing electronic data privacy and anonymity. In one example, the system may include at least one user device having a first privacy client operating on the user device; at least one service provider device having a second privacy client operating on the service provider device; and at least one privacy server coupled to the network, the privacy server communicating with the first and second privacy clients; wherein the privacy server includes an abstraction module that electronically links data attributes and attribute combinations and separates data attributes and attribute combinations, and the abstraction module associates a DDID with the data attributes and / or attribute combinations.

[0064] In one example, the privacy server may include an authentication module that generates and / or accepts one or more of said DDIDs. In another example, the privacy server may include a maintenance module that stores a combination of the DDIDs with their associated data attributes and / or attribute combinations. In another example, the privacy server may include a verification module that verifies the integrity of data attributes, attribute combinations, and DDIDs.

[0065] In another example, the privacy server may include an access log module that collects and stores information relating to the DDIDs and the data attributes for use in one or more post-incident forensic analyses in the event of one or more errors.

[0066] In one example, the DDID expires after a predetermined time, and after expiration of the DDID, the abstraction module assigns the DDID to another data attribute and / or to another Data Subject.

[0067] Other embodiments of the disclosure are described herein. The features, utilities and advantages of various embodiments of this disclosure will be apparent from the following more particular description of embodiments as illustrated in the accompanying drawings.

Brief Description of the Drawings

[0068]

Figure 1 illustrates an example of a block diagram of a system including a privacy server, in accordance with one embodiment of the invention.

Figure 1A illustrates an example of a block diagram of a system including a privacy server, in which the invention is offered as a service to interact with external databases in accordance with one embodiment of the invention.

Figure 1B illustrates different ways that assignment, application, expiration and recycling of DDIDs may occur with respect to data attributes and / or attribute combinations, in accordance with differing embodiments of the invention.

Figure 1C-1 illustrates potential input and output flows for a system including a privacy server from the perspective of a Trusted Party, in accordance with one embodiment of the invention.

Figure 1C-2 illustrates potential input and output flows for a system including a privacy server from the perspective of a Data Subject, in accordance with one embodiment of the invention.

Figure ID illustrates an example of the use of DDIDs in connection with a networked blood pressure monitor, in accordance with one embodiment of the invention.

Figure IE illustrates an example of the use of DDIDs in connection with serving patients with sexually transmitted diseases (STDs), in accordance with one embodiment of the invention.

Figure IF illustrates an example of the use of DDIDs in connection with offering a coupon, in accordance with one embodiment of the invention.

Figure 1G illustrates an example of the use of DDIDs in connection with a physician viewing blood pressure levels, in accordance with one embodiment of the invention.

Figure 1H illustrates an example using DDIDs to effect dynamic data obfuscation in connection education related

information, in accordance with one embodiment of the invention.

Figure 1I shows an example of a process to perform Disassociation Level Determination (DLD) and create an Anonymity Measurement Score (AMS), in accordance with one embodiment of the invention.

Figure 1J illustrates exemplary calculated Anonymity Measurement Scores, in accordance with one embodiment of the invention.

Figure 1K illustrates exemplary categories for the level of consent / involvement required by the Data Subject for certain calculated Anonymity Measurement Scores, in accordance with one embodiment of the invention.

Figure 1L illustrates an example of the use of DDIDs in the area of emergency response, in accordance with one embodiment of the invention.

Figures 2-4 illustrate an example of the generation and use of a TDR, in accordance with one embodiment of the invention.

Figure 5 illustrates two example attribute combinations having different levels of abstraction by means of the association function and the replacement function of the system, in accordance with one embodiment of the invention.

Figure 6 shows an example of a process (from a sample controlling entity and system perspective) to select attribute combinations, generate TDRs to abstract or anonymize the data, and then re-associate or de-anonymize the data, in accordance with one embodiment of the invention.

Figure 6A shows an example of a process (from a sample controlling entity and system perspective) to receive attributes from one or more external database, generate TDRs to abstract or anonymize the data, and then re-associate or de-anonymize the data, in accordance with one embodiment of the invention.

Figure 6B shows an example of a process (from a sample controlling entity and system perspective) to provide dynamic anonymity for data elements contained in one or more databases considered too sensitive to be revealed in an identifiable manner external to an organization.

Figure 7 shows an example of a process (from a recipient entity perspective) of the process of Figure 6, in accordance with one embodiment of the invention.

Figure 8 illustrates an example of a process for verifying authority, in accordance with one embodiment of the invention.

Figure 9 illustrates an example of a process for withholding key protection information unless verified, in accordance with one embodiment of the invention.

Figure 10 illustrates an example of a process for analyzing interests of related parties in an anonymous fashion, in accordance with one embodiment of the invention.

Figures 11-18 illustrate various examples of the interactions between a related party, service provider, and privacy server, including DDIDs and attribute combinations generated, sent, and tracked, in accordance with one embodiment of the invention.

Figure 19 shows examples of attribute combinations accessible to multiple service providers as well as the attribute combinations re-transmitted by each service provider back to a privacy server, in accordance with one embodiment of the invention.

Figure 20 shows the data accessible to a related party that includes all attribute combinations sent to and retransmitted from service providers, in accordance with one embodiment of the invention.

Figures 21 and 22 illustrate how a service provider acting as the controlling entity and providing information to various vendors, may provide to each vendor only those attribute combinations necessary to perform services assigned to it, in accordance with one embodiment of the invention.

Figure 23 illustrates an example of an implementation of DDIDs in the area of Internet advertising, in accordance with one embodiment of the invention.

Figures 24-25 illustrate examples of an implementation of DDIDs in the area of healthcare, in accordance with one embodiment of the invention.

Figure 26 illustrates an example of an implementation of DDIDs in the area of mobile communications, in accordance with one embodiment of the invention.

Figure 27 illustrates a block diagram of an example of a programmable device for implementing techniques for dynamically creating, assigning, changing, reassigning, and using dynamically changeable, temporally unique identifiers (DDIDs) in accordance with one embodiment of the invention.

Figure 28 illustrates a block diagram illustrating a network of privacy clients and a privacy server for implementing techniques for dynamically creating, assigning, changing, reassigning, and using DDIDs in accordance with one embodiment of the invention.

Detailed Description

[0069] Disclosed herein are various systems, methods and devices for private and secure management and use of information pertaining to one or more Data Subjects, such as persons, places or things, and / or associated actions,

activities, processes and / or traits. The systems, methods and devices described herein abstract data attributes pertaining to Data Subjects and / or associated actions, activities, processes and / or traits by linking data pertaining to Data Subjects and / or associated actions, activities, processes and / or traits to independent attributes and / or dependent attributes and separating elements pertaining to Data Subjects and / or associated actions, activities, processes and / or traits into independent attributes and / or dependent attributes. DDIDs can then be associated with select data attributes or select attribute combinations, thus creating TDRs. In this manner, embodiments of the present invention can be utilized to provide data security, privacy, anonymity, and accuracy for Data Subjects such as persons, places or things and / or associated actions, activities, processes and / or traits. Various embodiments of the present invention are disclosed herein.

Dynamic Anonymity / Circles of Trust (CoT)

[0070] Dynamic Anonymity is premised on the principle that static anonymity is an illusion, and that the use of static identifiers is fundamentally flawed. The Dynamic Anonymity system dynamically segments and applies re-assignable dynamic de-identifiers (DDIDs) to data stream elements at various stages (Note: while dynamic segmentation may include time lapse, it is more likely determined by activity, location and / or subject matter) thereby minimizing the risk of information being unintentionally shared in transit, in use or at rest, while maintaining the ability of Trusted Parties - and of no others - to re-stitch the data stream elements.

[0071] Cleartext primary keys may be used internally within a Circle of Trust ("CoT") such as shown in Figure 1C-1 to identify Data Subjects, actions, activities, processes and / or traits; however, these keys may not be shared outside the Circle of Trust. Rather, Dynamic Anonymity uses dynamically changing and re-assignable compound keys outside of a Circle of Trust which may be comprised of: (i) a DDID; and (ii) the time period / purpose for which the DDID is associated with a Data Subject, action, activity, process and / or trait). Information regarding this association may not be made available outside of the Circle of Trust (and it may not be reconstructible if the DDID representing a connection with one or more Data Subject, action, activity, process and / or trait contains no recoverable information leading back to said one or more Data Subject, action, activity, process or trait - in each such case, the connections would be severed and are not inherently computable).

[0072] Dynamic Anonymity enhances privacy, anonymity and personal data protection capabilities in distributed platforms / fragmented ecosystems, while providing superior access to, and use of, data in accordance with policies established by, or on behalf of, Data Subjects. In this manner, everyone - including those who elect to use either closed or distributed systems - benefits from enhanced data privacy and anonymity.

[0073] Dynamic Anonymity delivers certain immediate benefits without modification to existing business and technology practices. With the use of dynamically changing and temporally unique DDIDs, current systems and processes (e.g., web browsers and data analytic engines) may not recognize relationships between and among data elements. These systems and processes can process information using existing capabilities without creating inferences, correlations, profiles or conclusions except as expressly authorized by Data Subjects and trusted parties / proxies via a Circle of Trust (CoT). However, additional significant benefits would arise from new business and technology practices that leverage specific attributes and capabilities of DDIDs, Dynamic Anonymity and / or a Circle of Trust (CoT).

[0074] Dynamic Anonymity provides benefits at four distinct points of data processing:

A. Data Capture;
B. Data Transmission / Storage;
C. Data Analysis; and
D. Data Privacy / Anonymity Control.

At each point data is protected in accordance with PERMS specified by, or on behalf of, Data Subject(s) to whom that data pertains.

A. Data Capture

[0075] In applications where a static identifier would typically be associated with capture of data pertaining to a Data Subject, Dynamic Anonymity can provide:

1. A dynamic de-identifier (or DDID) that changes over time (triggered by a lapse of time, change in purpose, temporary cessation in activity, or change in virtual or physical location) limiting the ability to track, profile or otherwise associate data with a Data Subject, action, activity, process and / or trait.
2. An association from each DDID to the applicable one or more Data Subject, action, activity, process and / or trait, stored and known only within the applicable Circle of Trust (CoT).
3. Dynamic Anonymity also offers the optional ability to store data associated with DDIDs within a CoT.

[0076] A key feature of Dynamic Anonymity is the ability to anonymize and segregate data elements at the data element level rather than at the data record level - i.e., at the level of individual data elements associated with a Data Subject, action, activity, process and / or trait rather than data elements representing the entirety or majority of information pertaining to a Data Subject, action, activity, process and / or trait. Circles of Trust retain relationship information between and among data elements and Data Subjects, actions, activities, processes and / or traits to permit re-association according to privacy / anonymity policies and / or rules established by, and / or on behalf of, Data Subjects (referred to sometimes herein as PERMS).

Example: Search Engine

[0077] Consider a person who frequently uses a particular search engine. Currently, the search engine assigns the person (via their browser) a "cookie" or other digital footprint tracker that persists for months or years, against which an ever-increasing stream of observational data (e.g. search terms, links clicked, location data) is then accumulated and, very likely, analyzed and further aggregated by multiple parties - often revealing personally identifiable information without knowing consent by the Data Subject.

[0078] Dynamic Anonymity can leverage the natural response of a search engine to create a new cookie / digital footprint tracker for each Data Subject perceived to be interacting with the search engine for the first time. Clearing history, cache, cookie / digital footprint tracker, and associated data will cause the search engine to generate a new cookie / digital footprint tracker for the Data Subject. A Circle of Trust (CoT) can store information pertaining to associations of cookies / digital footprint trackers to the Data Subject, and optionally also store a list of queries and selected links.

[0079] With this approach, the search engine would still have access to aggregate data - trending search terms, popular websites, ad clicks, etc. - but would be prevented from drawing inferences related to the Data Subject based on observational data. If / as authorized by privacy / anonymity policies and / or rules established by, and / or on behalf of, the Data Subject, the CoT could enable the search engine to perform more detailed analysis. This could be implemented using an HTTP proxy or browser extension, requiring no modification to (or cooperation from) an existing search engine.

[0080] In the past, anonymous tracking cookies were supposed to have solved the problem of how to support both privacy and analytics. However, anonymous tracking cookies failed to achieve this goal because all the data was housed together and associated with random static identifiers that made it too easy to generate information that is linked or linkable to a Data Subject ("Personal Data" or "PD"), thereby nullifying or attenuating the value of the static "anonymous" identifiers. Dynamic Anonymity overcomes these shortcomings by employing dynamically changing and re-assignable DDIDs, storing the resulting DDID associations and obscuring keys within Circles of Trust, and providing a unique interaction model enabling participation between and among Data Subjects and Trusted Parties / third-party participants.

B. Data Transmission / Storage

[0081] A CoT is composed of one or more Trusted Parties, each of which may offer one or more independent data storage facilities, as well as secure means to segment and transmit sensitive data to these data stores.

[0082] Alternatively, Dynamic Anonymity-compliant application developers could choose to only store the Data Subject-to- DDID associations within the CoT, and instead to use Dynamic Anonymity-defined procedures to obscure, encrypt, and / or segment data (or utilize Dynamic Anonymity -enabled toolkits for such procedures); allowing applications to safely store generated or collected information in their own facilities, without loss of context or business value.

[0083] In the past, analogous techniques to those employed by the present invention have been employed to:

- Segment data;
- Encrypt and obfuscate data during transmission; and
- Employ distribution, obfuscation and security during storage.

However, Dynamic Anonymity improves upon these prior approaches by:

- Employing dynamically changing and re-assignable DDIDs to obscure data at the data element (versus data record) level;
- Storing resulting DDID associations / obscuring keys within a Circles of Trust; and
- Providing a unique interaction model for enabling participation between and among Data Subjects and Trusted Parties / third-party participants.

C. Data Analysis

[0084] Traditional techniques for data "cleansing" (also referred to as data cleaning and data scrubbing) paradoxically

suffer from two different and antithetical kinds of problems.

1. A given data cleansing technique can simply be ineffective. Despite earnest efforts, or even use of legally sanctioned techniques to obscure Personal Data, it may be still possible to identify the Data Subjects and Personal Data from "cleansed" data. Three famous examples:

   a. In the mid-1990s, the Massachusetts Group Insurance Commission (GIC) released data on individual hospital visits by state employees in order to aid important research. Latanya Sweeney, then an MIT graduate student, purchased the Cambridge voter-registration records, and by linking the two data sets, which individually were completely innocuous, she was able to re-identify then-Massachusetts Governor Bill Weld's GIC entry despite the fact that it had been "anonymized," with all obvious identifiers, such as name, address, and Social Security number, removed.
   b. In 2006, Arvind Narayanan, then a graduate student at UT-Austin, together with his advisor, showed that by linking the "anonymized" Netflix dataset to the Internet Movie Database (IMDb), in which viewers review movies, often under their own names, many Netflix users could be re-identified.
   c. In 2013, a team led by Dr. Yaniv Erlich, of the Whitehead Institute for Biomedical Research, re-identified men who had participated in the 1000 Genomes Project - an international consortium to place, in an open online database, the sequenced genomes of (as it turns out, 2500) "unidentified" people - who had also participated in a study of Mormon families in Utah.

2. More effective data cleansing techniques may reduce the business value of that data - that is, many obfuscation techniques are lossy.

[0085] The Dynamic Anonymity approach to data privacy / anonymity provides a way to avoid both pitfalls, simultaneously.

D. Data Privacy / Anonymity Control

[0086] In order to protect Personal Data, Dynamic Anonymity may employ a multiple means of measuring, specifying, and enforcing data privacy / anonymity:

1. A system for determining a privacy / anonymity level for each potential kind of exposure for data associated with a Data Subject, action, activity, process and / or trait. These privacy / anonymity levels may consist of a continuum of discrete values (between the extremes of complete privacy /anonymity and complete public exposure), and / or a mathematical specification of such (an "Anonymity Measure Score" or "AMS").
2. PERMS that specify actions allowed or limited by policies regarding data. (For example: "share," "update.")
3. PERMS that associate access levels, permissions and data with each other, thus granting or denying certain levels of access to data on the basis of one or more criteria, including data type, time, organization seeking access, etc.

[0087] A Data Subject's PERMS may also be combined with, or limited by, statutory policies. (For example, medical data in the US must be protected in accordance with the US Health Insurance Portability and Accountability Act (HIPAA.)
[0088] Additionally, if allowed by the Trusted Party and with the data owner's consent, offers to modify or grant specific and limited permissions may be presented to, and accepted by, Data Subjects.
[0089] Dynamic Anonymity may also improve upon existing frameworks by using privacy / anonymity level determinations to prevent inappropriate use of data, which is obscured and only analyzed, whether from inside or outside a Circle of Trust, in a manner consistent with each Data Subject's specified privacy / anonymity levels.

Dynamic De-Identifiers (DDIDs)

[0090] A dynamic de-identifier DDID is a temporally-bounded pseudonym which both refers to and obscures the value of (i) a primary key referencing a Data Subject, action, activity, process and / or trait, (ii) the value of an attribute of that Data Subject, action, activity, process and / or trait (e.g. a ZIP code), and/or (iii) the *kind or type* of data being associated with the Data Subject, action, activity, process and / or trait (e.g. the *fact* that some encoded value was a ZIP code).
[0091] DDIDs may additionally protect data if there is no discernable, inherent, nor computable relationship between their content and the values (cleartext) to which they refer. Additionally, the association between any given DDID and its cleartext value may not be exposed outside the Circle of Trust (CoT). Unlike static identifiers, an obscured value or key need not have the same associated DDID when used in a different context, for a different purpose, or at a different time.
[0092] DDIDs can be either generated within the Circle of Trust, or if the above criteria are satisfied, external IDs can

be used as DDIDs.

DDIDs are Time-Bounded

[0093] As mentioned, DDID associations are *temporally-bounded,* by which we mean that, even within the same context, and with regard to a single type of data (e.g. ZIP code), a particular DDID may refer to one value at one time, but may (if desired) also refer to another value at a different time.

[0094] This necessarily implies that in order to decode or expose the meaning of a particular DDID, an application must also retain knowledge of the time to which that DDID applied.

[0095] This knowledge may be *explicit* - that is, the assignment time may also be part of the record or document in which the DDID was stored - or it may be *implicit* - for example, an entire data set may have been obscured as a batch, and presumed (regardless of how long processing actually takes) to have occupied the same instant - and thus have only one consistent set of DDID mappings per field type. In order to reconstitute such data, one would also need to supply some reference to the corresponding set of DDID / value associations (stored within the CoT).

DDIDs are Purpose-Bounded

[0096] Note that DDIDs are also bounded by *context* or *purpose* - meaning the same DDID can recur in multiple contexts, even at the same time. For example, consider a stream of records, each of which contain a Social Security Number (SSN) and ZIP code, and which all occupy a single time block. In such a case, a particular DDID may be used both as a replacement for a ZIP code, and also as a replacement for an SSN.

[0097] As above, this implies that some indication of that context (e.g. was this a ZIP code or SSN?) will be necessary to obtain the cleartext to which that DDID referred.

Replacing Data with DDIDs

[0098] Consider the task of replacing a single stream of data - the same kind of data (e.g. ZIP codes or SSNs), occupying the same time block - with DDIDs. A (Java-like) "pseudocode" description of an Application Programming Interface (API) that carries out such behavior in one potential embodiment of the invention might look like this:

```
interface DDIDMap {
DDID protect(Value cleartext);
Value expose(DDID ddid);
}
```

[0099] In English, "interface" means that we're defining a collection of functions (named "DDIDMap") that operate on the same underlying data. Data types are here denoted with initial upper-case letters (e.g. "DDID"), and variable or function parameter names are denoted with initial lower-case letters (e.g. the "cleartext" function parameter must be data of type "Value" - where "Value" is just a stand-in for any kind of data which can be obscured: IDs, quantities, names, ZIP codes, etc.).

[0100] One function, "protect()", accepts some cleartext value and returns a corresponding DDID. If that value has been seen previously, its previously-assigned DDID will be returned. If it has not been encountered before, a new DDID (so-far unique to this data set) will be generated, associated with that value, and then returned.

[0101] The other function, "expose()", reverses this process: when a DDID is passed to it, it looks up and returns the cleartext value, which was previously encoded as that DDID. If the given DDID has never been seen before, it fails with an indication of error.

[0102] The data managed by these operations, then, is a two-way mapping from each cleartext value to the DDID that replaced it, and from the DDID back to the original value.

[0103] Note that although we've said that a given DDID can only refer to a single value, it **is** possible, if desired, to implement a variant version of this algorithm that allows a value to be associated with *more than one* DDID.

Managing DDID Maps by Time and Purpose

[0104] Recall that the above bidirectional DDID-to-value map operates (i) upon a single kind of data (that is, having the same type, context, and purpose), and (ii) within the same time block. In order to support operations across multiple times and contexts, we can posit another potential API which gives us the an appropriate DDID-to-value map for a given time and purpose:

```
interface DDIDMapManager {
DDIDMap getMap(Context context, Time time);
}
```

[0105] Here, "context" is (or emits) a key that refers to a particular kind of data being obscured. (Elsewhere in this document, sometimes also called the "association key" or "A_K".) For example, the context might be the name of the table and column in which data to be obscured will reside (e.g. "employee.salary"). It could also include other non-other chronological indications of purpose or scope.

[0106] The "time" parameter indicates the instant at which the DDID is being (or was) associated with its cleartext value. Since DDID-to-value maps span a *block* of time, and there are many time instances within a block, this implies there exists some function (used internally, within this API, thus not shown above) that finds the time block associated which each given time. (More on this in a moment.)

DDID Generation and Time-Blocking Strategies

[0107] Note that different kinds of data can employ different DDID replacement strategies. In addition to those mentioned in the next two sections, DDIDs can vary in size, whether they're universally unique or just unique to that data set (or time block), what kind of encoding they use (e.g., integers or text), etc. And although DDID generation should typically be random, one might also wish to employ deterministic or pseudo-random DDID generators for demonstration, testing, or debugging purposes.

Unique or Reused DDIDs

[0108] One potential strategy may allow a particular DDID to be assigned to two different Data Subjects in the same context, but during two different time blocks. For example, within the same collection of time-anchored records, the DDID "X3Q" might at one moment (in one time block) refer to (for example) "80228", and later (in another time block), "12124". (We'll call this strategy "DDID reuse.")

[0109] An alternative is to disallow such "reuse" - and stipulate that a given DDID, in the same context, can only refer to a single Subject. (Although the subject may still receive different DDIDs over time.)

[0110] The choice between these two strategies involves a tradeoff between increased obscurity and the ease with which one may perform aggregation queries on obscured data.

[0111] Imagine we wish to count patients per postal code. If postal codes DDIDs are unique, we can aggregate counts per DDID, and then ask the CoT to finish the query by resolving those DDIDs to their corresponding postal codes, and aggregating again. But if we have "reused" DDIDs, then we must send the entire list of DDIDs and corresponding times to the CoT for resolution (and aggregation) - because we can't be sure that two instances of the same DDID refer to the same value.

DDID Time Blocks

[0112] Implementations also have freedom to choose different strategies for segmenting DDID maps by time. Blocks of time may vary by size and / or time offset; sizes can be fixed, random, or determined by number of records assigned per time. (Note that employing an infinite-sized time block (for a given context) gives behavior equivalent to using "static" identifiers.)

Implementation

[0113] Although there may be many strategies for creating new DDIDs, the API for generating such DDIDs may look (essentially) identical, regardless of which strategy is implemented "under the hood".

[0114] For example:

```
interface DDIDFactory {
DDID createDDID();
}
```

[0115] Next, consider the task of determining what time block was associated with a given DDID assignment. Since a time block can contain many instances of time, we'll need some kind of a "time key" (sometimes abbreviated "T_K" in elsewhere in this document) to each time block. This implies the need for a function to obtain the appropriate key for any time instant:

```
TimeKey timeKey = getTimeKey(Time time);
```

[0116] Further, note that both time-blocking and DDID-generation strategies depend upon the *kind* of data which are being obscured. In short, they are both associated with a given "context" (which includes or implies a notion of data type and usage), meaning that the "Context" API must offer at least one function supporting each:

```
interface Context {
TimeKey getTimeKey(Time time);
DDIDFactory createDDIDFactory();
}
```

[0117] Given these two additional functions, we can imagine that the implementation of "getMap()" in "DDIDManager" (shown previously) may look something like this:

```
DDIDMap getMap(Context context, Time time) {
TimeKey timeKey = context.getTimeKey(time);
DDIDMap map = getExistingMap(context, timeKey);
if (map was not found) then
DDIDFactory factory = context.createDDIDFactory();
map = createMap(factory);
storeNewMap(context, timeKey, map);
endif
return map;
}
```

[0118] Here, "getExistingMap()" is some function that finds the map assigned to the given context and time key, "createMap()" creates a map which will use the given DDID factory, and "storeNewMap()" associates a newly-created map with the context and time key by which it will be retrieved later.)

Using Context to Obscure Data and Attribute Types

[0119] Dynamic Anonymity may define the following different kinds of data to be protected: (i) primary keys which refer to Data Subjects, actions, activities, processes and / or traits (e.g. employee ID), (ii) attribute data associated with, but not unique to, Data Subjects, actions, activities, processes and / or traits (e.g. employee postal code), and (iii) the indication of a disassociated (obscured) data element's *type,* itself (an "association key", or "A_K").

[0120] Each of these can be achieved by defining a different context: first we'll discuss (i) and (ii), which are both achieved by obscuring data values (replacing them with "replacement key" DDIDs, abbreviated as "R_K" elsewhere). We will address (iii) the indication of a disassociated (obscured) data element's type, below.

[0121] Consider a trivial example: an order table recording which customers bought products on a given day. Each record has a day number, a customer ID, and a product ID. We want to obscure this data for use or analysis by some third party, who is outside the CoT. In particular, we wish to obscure the customer and product IDs, but leave the day numbers intact.

[0122] To do so, we could create two "Context" instances: one for "Customer ID", and one for "Product ID". Although DDIDs, should ideally be random, for our purposes, let's assume that our "DDIDFactory" will create integer DDIDs sequentially, starting from 0. Further, assume that each DDID map spans only three days, so after three days, a new set of DDID mappings will be used. This also implies that DDIDs will be "reused" - the same DDID can refer to different values when used different blocks. (This is not an ideal encoding strategy and is used here only for illustration purposes.)

[0123] TABLE 1 show some cleartext sample data:

TABLE 1

Day	Customer ID	Product ID
1	500	ZZZ
2	600	XXX
3	600	YYY
4	700	TTT
5	500	YYY

(continued)

Day	Customer ID	Product ID
6	600	TTT

[0124] After being obscured (as specified above), this data would look as shown in TABLE 2 below:

TABLE 2

Day	Customer ID	Product ID
1	0	0
2	1	1
3	1	2
4	0	0
5	1	1
6	2	1

[0125] To understand this, you read down each column, and think in groups of three days (the first time block of DDIDs covers, for each obscured field, days 1-3, and the second covers 4-6).

[0126] For the first three days, customer ID is: 500, 600, 600. The resulting encoding is: 0, 1, 1 (note that 600 is repeated, so its DDID, 1, is also repeated.)

[0127] For the second three days, customer ID is: 700, 600, 500. And (starting over from 0), the result is: 0, 1, 2 (note that 500 was 0 before, now it's 2).

[0128] Product ID uses a separate context, and thus stream of DDIDs, so it also starts from zero:

For the first time block (XXX, YYY, TTT) becomes (0, 1, 2).
For the second time block (TTT, YYY, TTT) becomes (0, 1, 0).

[0129] Another "Context" could be employed to obscure the indication of a disassociated (obscured) data element's *type* (iii above), where the column names are examples of Attribute Keys (A_K)). This could be done using one DDID-to-value mapping for the whole set (effectively substituting DDID for the column names), or in time blocks (as with the other fields in this example) such that (if an appropriately random DDID generation strategy were employed) the affected records could not be analyzed without the assistance of the Circle of Trust.

Notes on Locality and Time

[0130] The example APIs defined above presume that when data is encoded, the encoding time is passed with each datum or record. This is only necessary when DDIDs are being "reused" within the same context (and thus time is needed to discriminate between the two potential meanings of that DDID). When a DDID is only assigned to one value per context, that DDID is sufficient to discover the (single) original value.

[0131] Time could also become an issue where "reused" DDIDs are being employed across different systems, which might have slightly different notions of time. If it is not possible to pass the time associated with a DDID encoding, a (chronological) "buffer" could be employed to prevent a DDID from being reused too close to it's original assignment. And when it is possible to pass the time associated with the data to be encoded, the time could be "sanity-checked" against the local system clock: skew within a small window (smaller than the DDID reuse buffer) could be tolerated, whereas larger differences would trigger an error report.

[0132] Finally, note that there is also flexibility regarding *where* data is being encoded: data could be streamed to a machine residing within the CoT, and then sent along to its destination after encoding. But, alternatively, the *encoding* portions of the above algorithms could be run *outside* the Circle of Trust, provided that the resulting DDID-to-value associations were (a) not stored on the local host, and (b) safely (e.g. using encryption, and with appropriate safeguards against data loss) streamed to a CoT host for persistence, lowering latency in critical applications.

Dynamic Anonymity: De-Identification without De-Valuation

[0133] "De-identification" techniques traditionally used in certain circumstances (e.g., HIPAA or health related circumstances) to protect data privacy / anonymity may be largely defensive in nature - e.g., a series of masking steps is applied to direct identifiers (e.g., name, address) and masking and / or statistically-based manipulations are applied to quasi-identifiers (e.g., age, sex, profession) in order to reduce the likelihood of re-identification by unauthorized third parties. This approach may result in a trade-offs between protecting against re-identification and retaining access to usable information.

[0134] Dynamic Anonymity may have significant offensive value in that the value of information can be retained and leveraged / exploited for authorized purposes, all with a statistically insignificant risk of re-identification of any datum. Dynamic Anonymity may reject the proposition and traditional dichotomy that, in order to minimize risk, one must sacrifice the value of information content. Instead, Dynamic Anonymity may minimize both risk and the amount of information lost, enabling most - if not all - of it to be recovered, but only upon authorization by the Data Subject / Trusted Party, not by unauthorized adversaries / "black hat" hackers.

[0135] Dynamic Anonymity may uniquely enable information to be used in different ways by multiple parties in a controlled environment that facilitates unlocking and maximizing the value of data. Dynamic Anonymity may maximize the value of potential business intelligence, research, analysis and other processes while simultaneously significantly improving the quality and performance of data privacy / anonymity processes.

[0136] When collected or stored, sensitive data may be "disassociated" from its subject using one or more of the following strategies, none of which incurs any loss in value:

1. Segmentation: Sensitive data may be split into several pieces, by data type, and transmitted and / or stored separately (either in separate Circles of Trust, or using different DDID mapping sets maintained by the same Trusted Party) so that each piece, alone, yields no Personal Data.
2. ID replacement: Static identifiers can be replaced with dynamically changing and re-assignable DDIDs obscuring the relationship between data and the Data Subject to which that data refers.
3. Obscuring: data values and data type indicators may also be replaced with DDIDs.

[0137] The DDIDs associated with these operations are stored within a Circle of Trust (CoT) as shown in Figure 1C-1; the original data may thus be reconstituted by reversing these transformations, but only with the cooperation of the CoT itself, and thus only when granted such permissions by, and / or on behalf of, the Data Subject.

[0138] Figure 1 illustrates an example of an embodiment of the invention, including a system having a privacy server 50 or privacy server module which securely manages various data attributes and data attribute combinations (which may include but are not limited to behavioral data, transaction histories, credit ratings, identity information, social network data, personal history information, medical and employment information, and education history) relating to a Data Subject for use in different applications 56. These applications 56 may include, but are not limited to:

- Healthcare Applications
  - Medical Records
  - Mobile Applications
  - Real-time Critical Care Applications
  - Regulatory Compliance (e.g., HIPAA)
  - Research
- Education Applications
  - Student Records
  - Research
- Mobile Applications
  - Geolocation (Beacons, GPS, Wi-Fi Fingerprinting)
  - Mobile Payment and Loyalty
- Financial Service Applications
  - Banking, Brokerage, etc.

- Payment Processing
- Payment Card Industry (PCI) Security
- Authorization
- Verification of card holder status
- Regulatory Compliance
- Research
- Credit assessment
- Fraud detection

◦ Web Applications

- Ad serving
- Content review
- E-commerce
- Social networks

◦ 'Internet of Things' Applications

- Telematics
- Smart Grid
- Smart Cities

• Traffic Monitoring
• Utility Monitoring

◦ Power
◦ Fuel
◦ Water/Sewage

• Waste Management

- Smart Offices
- Smart Factories
- Smart Homes

• Connected Entertainment

◦ TV
◦ Streaming Devices

• Automation

◦ HVAC
◦ Lighting

• Security

◦ Window / Door Locks
◦ Fire / Smoke / Carbon Monoxide Detectors

• Appliances

- Smart Vehicles
- Agriculture-Field Sensors
- Wearable Devices

• Healthcare Monitoring
• Fit devices

- Eyewear
- Clothing

- Drones

◦ Private Wireless/Wired Networks

- Crop Sensors
- Tagged Animal Tracking
- Troop Movements

◦ Private Security Applications
◦ E-Commerce Applications
◦ Offline Retail Applications
◦ Human Resources/Hiring Applications
◦ Governmental Applications
- National Security Applications

- Analysis of call detail records
- Analysis of web browsing behavior
- Analysis of online and offline purchasing behavior
- Analysis of travel behavior
- Analysis of social media activity
- Analysis of circles of friends, acquaintances and other relationships

◦ Attorney/Law Firm Applications
- Maintaining of confidentiality/attorney-client privilege

◦ Consumer Contest Entry Applications
◦ Dating Applications
◦ Gambling and e-Wagering Applications

[0139] Figure 1A illustrates an example of an embodiment of the invention, including a system having a privacy server 50 or privacy server module which receives electronic data from one or more external databases 82 and securely converts various data attributes and data attribute combinations from such one or more external data bases (which may include but are not limited to behavioral data, transaction histories, credit ratings, identity information, social network data, personal history information, employment information, medical and education history) relating to a Data Subject into TDRs for use in different applications. Alternatively, applications store only Data Subject-to-DDID association information within the privacy server 50 and use Dynamic Anonymity-defined procedures to obscure, encrypt, and / or segment data stored in external databases 82. In this manner, Data Subject-to-DDID association information stored within the privacy server 50 could provide greater context and / or business value to information generated, collected and / or stored in external databases 82.

[0140] In one example, embodiments of the invention may form a secure and comprehensive aggregated data profile 58 of a Data Subject for use in one or more applications 56. A Data Subject or related party thereto, e.g., user 59, may anonymously communicate or selectively disclose the Data Subject's identity and / or data attributes from the Data Subject's aggregated data profile 58 (comprised of data attributes, attribute combinations or portions thereof, potentially from unrelated data sources) to vendors, service providers, advertisers or other entities with whom the Data Subject or related party is interested in communicating 57 via a network 72 (for instance, to possibly receive services or enter into a purchase transaction) based on one or more of the Data Subject's characteristics as expressed in the Data Subject's aggregated data profile 58 (comprised of data attributes, data attribute combinations or portions thereof, potentially from unrelated data sources). In this manner, embodiments of the invention provide for digital rights management for individuals ("DRMI") referring to a Data Subject, a related party or a third party managing data attributes and data attribute combinations pertaining to a Data Subject or digital rights management for de-identification ("DRMD") comprised of a third party managing data attributes and data attribute combinations associated with one or more Data Subjects. In one example, the extent to which information regarding the data attributes, data attribute combinations, Data Subjects and / or related parties may be made available to other parties may be controlled by embodiments of the present invention.

[0141] In the examples of Figure 1 and Figure 1A, a plurality of users 59, for example Data Subjects or service providers, utilize devices such as smart devices 70 (e.g., wearable, mobile or immobile smart devices), smartphones, tablets, notebooks, desktop computers, wired or wireless devices, or other computing devices running a privacy client application

60 to access a network 72 such as the Internet. As shown in Figure 1 and Figure 1A, a system 80 is illustrated which is coupled with and in communication with the Internet or other public or private network, and the system may include a privacy server 50 securely coupled with one or more databases 82. In one example, the privacy server 50 may be implemented using computer program modules, code products, or modules running on a server or other computing device. The one or more databases 82 may be implemented using any conventional database technology, including technology that securely stores data (such as through encryption) in redundant locations such as but not limited to RAID storage devices, network attached storage, or any other conventional databases.

[0142] In one example, the privacy server 50 implements one or more of the operations, processes, functions or process steps described herein, and the privacy server 50 may include or be configured to include other operations, functions or process steps as desired depending upon the particular implementation of the invention, including but not limited to the following processes, operations or functions performed by the indicated modules:

[0143] An authentication module 51 that may provide for both internal and external authentication including the following processes:

a. Internal authentication of privacy client 60 requests for TDRs, and privacy server 50 generation of TDRs.
b. External authentication before allowing participation in desired actions, activities, or processes and use of TDRs to authenticate recipients as approved to receive Time Keys (TKs), Association Keys (AKs) and / or Replacement Keys (RKs) as may be necessary to unlock contents of TDRs.
c. One example implementation of the authorization module may include allowing delegation of the ability to request generation of DDIDs and associated TDRs to other parties authorized by the controlling entity.

[0144] An abstraction module 52 that may provide internal and external abstraction that may include one or more of the following processes:

a. Selecting DDIDs by means of generating unique DDIDs or accepting or modifying temporally unique, dynamically changing values to serve as DDIDs.
b. Associating DDIDs with data attributes or attribute combinations to form TDRs for given Data Subjects, actions, activities, processes or traits.
c. Including only a portion of relevant data attributes in TDRs thereby disassociating the data attributes pertaining to a Data Subject and / or relevant for a given action, activity, process or trait.
d. Replacing one or more of data attributes contained in one or more TDRs with DDIDs.
e. Replacing with DDIDs one or more references to external networks, internets, intranets, and / or computing devices that may be integrated, or communicate, with one or more embodiments of the present invention.

[0145] A maintenance module 53 that may store:

a. TDR information pertaining to Data Subjects, actions, activities, processes or traits, "Pertinent Data" (defined as data initially associated with a DDID and / or data aggregated with a DDID during and / or following the time period of association) and / or DDIDs; and
b. Key information pertaining to (a) Time Keys (TKs) reflecting information regarding the time periods during which each DDID was associated with a particular Data Subject, attribute, attribute combination, action, activity, process or trait, (b) Association Keys (AKs) and / or (c) Replacement Keys (RKs); Thereby allowing the TDRs to be later re-associated with a particular attribute, attribute combination, action, activity, process, trait and / or associated Data Subject. In addition, the maintenance module may perform further analysis and processing of attributes, or attribute combinations in a secure environment.

[0146] An access log module 54 that may include collecting and storing information to enable post-incident forensic analysis in the event of system error and / or misuse.

[0147] A verification module 55 that may include validating and verifying the integrity of aggregated data profiles including data attributes, attribute combinations, DDIDs, and TDRs at any point in time.

[0148] As described herein, embodiments of the present invention are directed to promoting privacy, anonymity, security, and accuracy in relation to electronic data and network communication, analysis and / or research. In one example, data elements pertaining to Data Subjects, actions, activities, processes or traits may be abstracted by linking data elements pertaining to the Data Subject, action, activity, process or trait to independent attributes or dependent attributes and / or separating data elements pertaining to the Data Subject, action, activity, process or trait into independent attributes or dependent attributes. For purposes of this disclosure, a data attribute may refer to any data element that can be used, independently or in combination with other data elements, to identify a Data Subject, such as a person, place or thing, and / or associated actions, activities, processes or traits.

[0149] As mentioned above, in addition to abstracting data that may be used to identify Data Subjects such as a person, place or thing, the abstraction module 52 of Figure 1 or Figure 1A may also be used to abstract data related to Data Subjects such as things which may include, but are not limited to: physical or virtual things and entities; hardware or virtual devices; software applications; legal entities; objects; images; audio or video information; sensory information; multimedia information; geo-location information; privacy / anonymity information; security information; electronic messaging information including senders and receivers, message content, hyperlinks in messages, embedded content in messages, and information relating to the devices and servers involved in sending and receiving the messages; social media and electronic forums; online websites and blogs; RFID (radio frequency identification); tracking information; tax information; educational information; identifiers related to military, national defense, or other government entity programs; virtual reality information; massively multiplayer online role-playing games (i.e., MMORPGs); medical information; biometric data; behavior metric information; genetic information; data referring to the physical or virtual location of other data; and instantiations or representations of data or information.

[0150] The systems, methods and devices described herein may be used in one example to provide digital rights management for an individual (DRMI) and / or digital rights management for de-identification (DRMD). Digital rights management for an individual may comprise individual directed privacy / anonymity wherein a related party manages data attributes pertaining to one or more related parties. In this situation, the related party would serve as the controlling entity. Alternatively, a third party may manage data attributes pertaining to one or more related parties thereby comprising entity directed privacy / anonymity. In this situation, the third party would serve as the controlling entity. Digital rights management for de-identification also comprises entity directed privacy / anonymity, wherein a third party manages data attributes associated with data attributes associated with related parties, and controls the extent to which information regarding the data attributes and / or related parties is made available to other parties.

[0151] The systems, methods and devices disclosed herein may be used to provide DRMI such that one or more related parties, directly or indirectly, may manage their online digital fingerprint of data. The related parties may also control the extent to which information pertaining to data attributes, Data Subjects or one or more related parties is made available to third parties, such that the information and data may be made available in an anonymous, non re-identifiable manner. The systems, methods and devices provide a dynamically changing environment in which related parties may want to share data at one moment but not at the next moment. This is done with the understanding that the time intervals, specific receiving entities, physical or virtual whereabouts, or other mechanisms that trigger changes in the data to be shared may be dynamic in nature. Implementing DRMI enables non re-identifiable anonymity, and may allow for different information pertaining to data attributes, Data Subjects and related parties to be shared for different purposes on a dynamically changing, time and / or place sensitive, case-by-case basis. Particular needs with respect to information pertaining to data attributes, Data Subjects or related parties at specific times and places may be accommodated without revealing additional, unnecessary information, unless such revealing is authorized by the controlling entity. Additional, unnecessary information may be, for example, the true identity of the Data Subject or related party, mailing addresses, email addresses, previous online actions, or any other information not necessary for an unrelated party with respect to a specific action, activity, process or trait with respect to a Data Subject or related party.

[0152] The systems, methods and devices disclosed herein may be used to provide DRMD such that entities may centrally manage the online digital fingerprint of information pertaining to data attributes, Data Subjects and related parties for which they are responsible; and such entities may control the extent to which information is made available to other parties in a non re-identifiable versus identifiable manner. This allows the entity to satisfy de-identification objectives and / or obligations to comply with desires of Data Subjects, related parties and regulatory protections and prohibitions.

[0153] Example implementations of some embodiments of the invention can be configured to provide DRMI and / or DRMD capabilities with regard to data attributes comprised of images or video files revealing identifying facial characteristics are discussed below. A Data Subject or related party may benefit from others being able to make inferences about identity based on unique facial characteristics of the Data Subject in an electronic image. However, the rapidly expanding commercial availability and use of facial recognition technologies combined with the growing availability of electronic images pose issues with regard to privacy / anonymity and security of Data Subjects and related parties. In one example, privacy / anonymity and security can be safeguarded using one or more aspects of the present disclosures, with respect to Data Subjects and related parties, in the context of data attributes that are photos including facial images and characteristics of Data Subjects.

[0154] In some embodiments, the systems, methods and devices disclosed herein can be configured to distinguish between the status of parties as registered / authorized versus nonregistered / unauthorized visitors to a website or other electronic image-sharing application containing a data attribute. A distinction may also be made between registered / authorized visitors to a website or other photo sharing application containing data attributes pertaining to contacts / friends of a Data Subject or related party versus not contacts / friends of a Data Subject or related party depending on the status of a party. In one example, a system of the present invention may control whether any image data attribute is presented containing facial features. If an image data attribute is presented containing facial features, the system may

further control and limit unauthorized use and copying of photos that can lead to unintended secondary uses through additional protection techniques. In addition, some embodiments of the present invention may provide Data Subjects, related parties and controlling entities with the ability to designate which additional parties and for which specific purposes the image data attribute may be presented at all. If the data attribute is presented, the Data Subjects, related parties or controlling entities may designate whether the image makes use of known protection techniques aimed at limiting unauthorized use and copying of photos, thereby preventing or reducing the risk of unintended secondary uses of the image.

[0155] DRMI may enable Data Subjects and related parties, directly or indirectly, to manage photos containing facial images and control the extent to which photos pertaining to the related parties are made available to third parties in an identifiable, non-identifiable, reproducible or non-reproducible manner.

[0156] An example of a potential implementation of the present invention may involve use of DRMI by a provider of wearable, implantable, embeddable, or otherwise connectable computing technology / devices to mitigate potential public concern over information obtained and / or processed using the technology / device. For example, GOOGLE® could adopt DRMI to facilitate wider adoption of GOOGLE GLASS® by establishing a do-not-digitally-display-list (analogous to the do-not-call-list maintained by the FTC to limit undesired solicitation calls to individuals) that enables Data Subjects or related parties to register to prohibit the digital display of unauthorized photos taken using or displayed by GOOGLE GLASS®. (GOOGLE® and GOOGLE GLASS® are trademarks of Google, Inc.)

[0157] DRMI provided by one example of the present invention may further provide a Data Subject or related party who is a member of the professional networking site LinkedIn.com with a feature to manage the extent to which photos are made available to third parties in an identifiable, non-identifiable, reproducible or non-reproducible manner. Access to, use of, and copying of photos containing facial images of a Data Subject or related party may be controlled using, in one example, a three-tiered categorization schema:

Category A treatment or status may apply to visitors to the LinkedIn.com website who are not registered / authorized members of LinkedIn.com. These visitors may be provided no means to view or copy photos containing facial images of registered/authorized LinkedIn® (LinkedIn® is a trademark of LinkedIn Corporation.) members. Instead, they may be served via their web browser, mobile application or other application a graphic, image, indicator or avatar that indicates photos are available only to registered/authorized users of the LinkedIn.com website.

Category B treatment or status may apply to registered / authorized members of LinkedIn.com who are not authenticated contacts of a registered / authorized member of LinkedIn.com. By using additional protection techniques aimed at limiting unauthorized use and copying of photos that can lead to unintended secondary uses, these registered / authorized members may be provided with limited means to view or copy photos containing facial images of LinkedIn® member with regard to whom they are not an authenticated contact. These additional protection techniques may include but are not limited to:

1. Tiling to divide an image into smaller image tiles that will appear as a continuous image but are limited to only one tile piece at a time with respect to any entity endeavoring to copy the image;
2. Employing image watermarking techniques;
3. Hiding layers to place an image containing facial characteristics behind a transparent foreground image;
4. Providing images without a color profile or palette;
5. Preventing downloads through table instructions that disable 'right click' copying or use of images;
6. Preventing downloads through JavaScript technology that disables 'right click" copying or use capabilities images;
7. Preventing downloads through Flash technology that disables 'right click" copying or use capabilities images;
8. Hiding images by URL encoding techniques images;
9. Using META tags to prevent images containing facial features from being indexed by search engine spiders, robots or bots images; and
10. Using Robot.txt files to prevent images containing facial features from being indexed by search engine spiders, robots or bots images.

Category C treatment or status may apply to registered / authorized members of LinkedIn.com who are also authenticated contacts of another registered / authorized member of LinkedIn.com. These registered / authorized members may be provided with full means to view or copy photos containing facial images of the other LinkedIn® member.

[0158] DRMD may be provided by some example of the present invention such that entities can centrally manage photo data attributes containing facial images for which they are responsible and can control the extent to which the photo data attributes are made available to other parties in an identifiable, non-identifiable, reproducible or non-repro-

ducible manner.

[0159] One example of a potential implementation of the present invention may involve use of a system providing DRMD by a controlling entity that leverages known facial image recognition capabilities to limit disclosure of elements by parties who are not authorized by a Data Subject or related party of a photo data attribute which contains recognizable facial elements of said registered / authorized Data Subject or related party to view the facial elements. Rather, a party who tries to upload, use or view a photo that includes facial elements of a registered / authorized Data Subject or related party whose facial characteristics are registered with the DRMD system, but which party has not been authorized by the registered / authorized Data Subject or related party, may see and be able to use only a modified version of the photo altered by the DRMD system to block out or 'de-tag' the recognizable facial elements of the registered / authorized Data Subject or related party. For example, a picture taken at a public bar that includes the face of a Data Subject or related party registered with a system providing DRMD may be modified to block out or 'de-tag' the face of the related party on all versions of the photo except those as explicitly authorized by the Data Subject or related party.

[0160] In one example of the present invention, the authentication module can be configured so that decisions as to who sees what information are determined by a controlling entity on a configurable basis. In one example, the configurable control may include automatic and / or manual decisions and updates made on a timely, case-by-case manner by providing each controlling entity with the ability to dynamically change the composition of information comprised of data attributes at any time. The enhanced customization achieved by dynamically changing the composition of data attributes leads to greater relevancy and accuracy of information offered pertaining to a data attribute and / or related party. As disclosed herein, use of DDIDs as a component of privacy, anonymity and security enables each recipient entity receiving information to receive different information as appropriate for each particular purpose, thereby fostering the distribution of fresh, timely and highly relevant and accurate information, as opposed to stale, time burdened, less accurate accretive data such as provided via conventional persistent or static identifiers or other mechanisms.

[0161] Figure 1 and Figure 1A also illustrate various examples of privacy clients 60 operating on user devices 70 such as computers, smartphones or other wired or wireless devices, wherein the user devices may communicate with the privacy server 50 over a network 72 such as the Internet or other public or private network.

[0162] In one example, a privacy client component of the present disclosure may be resident on a mobile device. The privacy client may be provided as part of a mobile application or operating system running on the mobile device, or may be configured as a hardware device, integrated circuit or chip of a mobile device. Mobile devices implementing one or more aspects of the present disclosure may possess real-time knowledge of location, activity and / or behavior with respect to Data Subjects and / or related parties pertaining to the device. The mobile device may also transmit, receive and process information with other devices and information sources. Mobile applications interacting with the privacy client may provide the controlling entity with control over both the timing and level of participation in location and time sensitive applications, and the degree to which information is shared with third parties in an anonymous-rather than personally identifiable-manner. Mobile devices implementing one or more aspects of the present disclosure may also leverage the unique capabilities of mobile devices to aggregate a user's personal preference information gathered from across a variety of unrelated and disparate sources (whether they be mobile devices, more traditional computer systems or a combination of both) and-only with the users' approval-share a user's information (on an anonymous or personalized basis) with vendors to facilitate time- and / or location-sensitive personalized commercial opportunities. As may now be understood more clearly, users may determine whether the benefits of such time- and / or location-sensitive personalized commercial opportunities justify identifying themselves in connection with the transactions.

[0163] For example, without embodiment of the invention, static identifiers conventionally associated with a mobile device may enable mobile application providers and other third parties to aggregate information pertaining to use of the mobile device; and by aggregating the data on use of the mobile device, application providers and other third parties may obtain information which may include but not be limited to information related to the device user's frequent physical locations, calling habits, content preferences, and online transactions that they could not obtain through data from any one time interaction with the device user. Through the use of some embodiments of the present invention, application providers and other third parties would be prevented from aggregating information pertaining to use of a mobile device by Data Subjects and related parties; and some embodiments of the present invention may be configured to provide a mobile device with use mobile applications requiring access to geolocation information (e.g., direction or map applications), without revealing the identity of the mobile device, Data Subject or related party by means of dynamically created, changeable and re-assignable DDIDs described herein; rather than conventional static identifiers.

[0164] In one example, embodiments of the present invention may be configured to provide enhanced privacy, anonymity, security and accuracy over persistent and / or static identifiers, and by leveraging DDIDs rather than aggregate on a static identifier; thereby, embodiments of the present invention can provide a solution to online digital fingerprints being left across networks and internets. As a result, embodiments of the present invention may provide a controlling entity with the ability to decide who sees what data, prevent data aggregators from understanding data connections pertaining to a Data Subject or related party without the controlling entity's permission, and provide control to the controlling entity over upstream and / or downstream dissemination of information.

[0165] In one example of the present invention, continued access may be provided for the benefits of big data analytics by using DDIDs to provide multiple protective levels of abstraction. Systems, methods and devices embodying some aspects of the present invention also do not suffer from the fundamental flaws of Do-Not-Track and other initiatives that eliminate access to the data required for effective big data analytics and that are inconsistent with economic models offering free or discounted products or services in return for information. Do-Not-Track is a technology and policy proposal that enables Data Subjects or related parties to opt out of certain tracking by websites and third party data collecting entities as they are online, including analytics services, advertising networks, and social platforms. Although Do-Not-Track provides Data Subjects and related parties with enhanced privacy, anonymity and security, it denies them the benefits of receiving customized, personally relevant offerings while online through big data analytics. This impacts the economic benefits that big data analytics provides to merchants, service providers, and Data Subjects or related parties themselves.

[0166] In contrast, some embodiments of the present invention may have a net neutral to positive revenue impact (versus the net negative revenue impact of Do-Not-Track initiatives), because with some embodiments of the present invention, a controlling entity may include data attributes in TDRs that enable recipient entities to use existing tracking technology to track TDRs for the duration of their existence. The controlling entity may also include information that is more accurate than available via tracking alone to facilitate personalization and customization. For example, a controlling entity may elect to include certain data with regard to past browsing sessions on a website in the attribute combinations pertaining to a Data Subject or related party that are sent via a privacy client to that website, augmented with other specific more up-to-date information beneficial to both the website and the Data Subject or related party.

[0167] Referring to Figure 1 and Figure 1A, one embodiment of the present invention may comprise a computer network 72 in which one or more remote privacy clients 60 comprised of computer hardware, firmware or software resident on one or more computing devices 70 or resident on and accessible via a network device send requests/queries to, and receive services/responses from, one or more computing devices that act as privacy servers 50. Privacy client computing devices 70 may comprise smart devices (i.e., wearable, movable or immovable smart devices), smartphones, tablets, notebook computers, desktop computers, or other computing devices with programs that (i) enable requests for services from, and / or submission of queries to, privacy servers, (ii) provide user interface capabilities, (iii) provide application processing capabilities, and / or (iv) offer localized storage and memory. Privacy server 50 computing devices may comprise large personal computers, minicomputers, mainframe computers or other computing devices with programs that (i) respond to requests for services/queries from privacy clients, (ii) provide centralized or decentralized administration of the system, (iii) provide high-volume application processing capabilities, and / or (iv) offer high-volume storage and memory capabilities integrated with one or more databases. Privacy servers 50 may also be configured to perform one or more of the operations or features described herein. Communications capabilities between and among privacy servers and privacy clients may be comprised of computer networks, internets, intranets, public and private networks or communication channels, and supporting technologies.

[0168] Referring to Figure 1 and Figure 1A, another potential embodiment of the present invention may comprise a computer network in which one or more remote privacy clients 60 comprised of computer hardware, firmware or software resident on one or more computing devices 70 or resident on and accessible via a network device-send requests / queries to and receive services/responses from, one or more computing devices that act as privacy servers 50 wherein said privacy servers 50 may transmit via the Internet, internets, intranets or other networks electronic information to cards, mobile, wearable and / or other portable devices that may include means of electronically receiving and storing information, wherein said cards, mobile, wearable and / or other portable devices contain information pertaining to data attributes and / or DDIDs until such time, if any, as said information pertaining to data attributes and / or DDIDs is modified by said privacy servers.

[0169] The privacy servers and privacy clients may implement modules including program code that carry out one or more steps or operations of the processes and / or features described herein. The program code may be stored on a computer readable medium, accessible by a processor of the privacy server or privacy client. The computer readable medium may be volatile or non-volatile, and may be removable or non-removable. The computer readable medium may be, but is not limited to, RAM, ROM, solid state memory technology, Erasable Programmable ROM ("EPROM"), Electrically Erasable Programmable ROM ("EEPROM"), CD-ROM, DVD, magnetic cassettes, magnetic tape, magnetic disk storage, other magnetic or optical storage devices, or any other conventional storage technique or storage device.

[0170] Privacy servers and associated databases may store information pertaining to TDRs, time periods / stamps, DDIDs, attributes, attribute combinations, Data Subjects, related parties, associated profiles and other related information. Privacy servers and associated databases may be managed by and accessible to the controlling entity, but, in one example, not by other parties unless authorized by the controlling entity. In one example, an authentication module of one or more privacy servers controls access to data through the TDRs. Privacy clients may request information from privacy servers necessary to perform desired actions, activities, processes or traits and / or query privacy servers whether TDRs are authorized to participate with respect to a requested action, activity, process or trait at a particular time and / or place. Privacy clients may also aggregate data with respect to actions, activities, processes or traits in which TDRs

associated with the privacy client engage, such as tracking data, obviating the need to return to the database for data extrapolation. Insights gleaned by other parties may become part of a TDR for its duration, in one example.

[0171] In one example implementation of the invention, the abstraction module 52 is configured such that a controlling entity (which may be the Data Subject or a related party) links data pertaining to a Data Subject to attributes and / or separates data pertaining to a Data Subject into attributes that can be divided, combined, rearranged, or added into various attribute combinations. These combinations may contain any combination of attributes or previously created attribute combinations associated with the Data Subject.

[0172] In this example with regard to each intended action, activity, process or trait involving the privacy server, the abstraction module in one example enables the controlling entity to limit the degree of identifying information transmitted or stored by selecting from among the attributes only those that are necessary with respect to a desired action, activity, process or trait and linking those data attributes to one or more attribute combinations and / or separating those data attributes into one or more attribute combinations. The controlling entity may then use the abstraction module to dynamically create and / or assign a DDID to form a TDR for each attribute combination. The DDID may be configured to expire after preset delays or cues, and may be re-used for data associated with another action, activity, process or trait and / or other Data Subjects or related parties, thereby leaving no precise trail of association outside of the privacy server. In one example, before assigning or accepting a DDID to form a TDR, the abstraction module may verify that the DDID is not actively being used in another TDR. In order to make this verification, an additional buffer timeout period may be included to address potential outages and system down time. The greater the number of data attributes and associated TDRs generated with respect to a desired action, activity, process, or trait, the greater the privacy, anonymity, and security achieved. In this situation, an unauthorized party gaining access to one of the TDRs would gain access to only that information contained in the TDR. In one example, the information in a single TDR may be only a fraction of the attributes necessary with respect to the desired action, activity, process, or trait, and further does not provide the information necessary to determine other TDRs containing necessary attributes, or to determine any Data Subjects and / or related parties that may be associated with the TDRs.

[0173] In one example, the creation of TDRs by means of the abstraction module may be based on one or more processes that match prescribed steps necessary to describe or perform different actions, activities or processes with specified categories of attributes associated with the steps, and selecting or combining those attributes necessary with respect to the particular action, activity, process or trait. The process of creating TDRs by means of the abstraction module may be performed directly by the controlling entity or indirectly by one or more parties authorized by the controlling entity.

[0174] For example, a first database containing credit card purchasing information may include information necessary for a credit card issuer to conduct big data analytics on the purchasing information. However, the database need not include identifying information for the users of the credit cards. Identifying information for the users of the credit cards could be represented in this first database by DDIDs, and the Replacement Keys (RKs) necessary to associate the DDIDs with the users could be stored in a separate secure database accessible to a privacy server and / or system modules. In this manner, the system may help protect the identity of credit card users and limit potential financial loss in the event of unauthorized entry into the first database containing credit card purchasing information because the DDIDs and related information would not be decipherable to unauthorized parties.

[0175] In addition, in one example of the present invention, real-time or batch analysis of data from mobile / wearable / portable devices can be performed in a manner that would be beneficial to receiving entities, such as merchants or service providers, without sacrificing the privacy / anonymity of the users of the mobile / wearable / portable devices. Each user may be considered a related party to the mobile / wearable / portable device in question as well as the Data Subject associated with the device itself or use of the device. In return for special offers or other concessions proffered by receiving entities, users of the mobile / wearable / portable devices could elect to have non-identifying TDRs shared in an anonymous fashion based on the users' real-time location, real-time activities, or during a particular temporal period, e.g., with receiving entities that are located within a prescribed distance of a particular geographic location (e.g., 1 mile, 1000 feet, 20 feet, or other distance depending upon the implementation) or within a prescribed category (e.g., jewelry, clothes, restaurant, bookstore, or other establishment) with respect to the location of the mobile / wearable / portable device. In this manner, receiving entities could have an accurate aggregated view of the demographics of their potential customer base-in terms of age, gender, income, and other features. These demographics may be revealed by TDRs shared by the mobile / wearable / portable device users at different locations, times of the day and days of the week that may help receiving parties more effectively determine what services, desired inventory and other sales, supply chain, or inventory-related activities to offer with regard to related parties. In one example, Data Subjects and related parties, which may be the users of the mobile / wearable / portable devices, would benefit from special arrangements or offers without ever having to reveal their personal information to the receiving entities (who would simply know that a Data Subject or related party was registered, but would not know what specific information to associate with any particular Data Subject or related party) unless and only to the extent desired by the Data Subject or related party.

[0176] In one example implementation of the invention, the authorization module can provide the controlling entity

with control over which other entities may be provided access to, or use of, TDR information. The controlling entity may further use the abstraction module to control the degree to which the other entities have access to specific elements of information contained in the system. For example, a mobile / wearable / portable platform provider serving as the controlling entity may provide performance data to a mobile / wearable / portable device manufacturer without having to reveal the identity of the device, Data Subject or related party user or location of the device, Data Subject or related party user. The mobile / wearable / portable platform provider may also provide a mobile / wearable / portable application provider with geolocation data necessary for a mobile / wearable / portable device to use a mapping or other application without having to reveal the identity of the device, Data Subject or related party user. Conversely, the mobile / wearable / portable platform provider may use the system to provide an emergency 911 system with location and identity data pertaining to the device as well as the Data Subject or related party user of the device. One example implementation of the authorization module may include allowing delegation of the ability to request generation of DDIDs and associated TDRs to other parties authorized by the controlling entity.

[0177] According to one example implementation of the present invention, receiving entities could use information regarding mobile / wearable / portable device related parties to customize user experiences or opportunities at locations where related parties gather, without requiring that personal identifying information be revealed. For example, a band that plays both country-western and gospel music could, in real-time or near real-time, determine that the majority of related parties attending the concert preferred gospel music and adjust their song selection for the concert accordingly by receiving TDRs related to the Data Subjects or related parties that are concert attendees. Similarly, in stores using video screens to display merchandise or special offers, store management could know in real time when they have a large presence of customers of a particular demographic in the store by receiving and analyzing TDRs associated with Data Subjects or related parties that are customers from clients in mobile / wearable / portable devices. The store could then play videos targeted to that particular demographic, and change the videos throughout the day in response to changes in the demographics of Data Subjects or related parties as communicated to the store system via clients in mobile / wearable / portable devices. The demographics obtained from information in the TDRs may include, but are not limited to, age, gender, or level income of Data Subjects or related parties. Similarly, in retail stores using real-time geolocation to identify a given customer's specific location in the store, special discounts or offers could be made to a customer that is a Data Subject or related party via their mobile phone, tablet or wearable device by receiving and analyzing TDRs associated with the Data Subject or related party's personal tastes, brand preferences and product buying preferences, where such TDRs would also include exogenous information added in real-time based on the products available to that Data Subject or related party at the location in the store at which they are present.

[0178] In one example implementation of the invention, the abstraction module of the privacy server assigns DDIDs to attribute combinations necessary to fulfill requests by and / or queries from privacy clients that may reside in numerous locations including but not limited to on Data Subject devices, on service provider devices, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server thereby creating TDRs for the period of the association between the DDID and the desired attribute combinations. The TDR in a privacy client may interact freely with a recipient entity for the configured time, action, activity, process or trait. Once a period of interaction with a designated recipient entity is completed, the privacy client may in one example return the TDR augmented by attribute combinations pertinent to activity of the privacy client to the privacy servers and associated databases. The privacy server may then associate various attribute combinations back with particular Data Subjects, as well as update and store the attribute combinations in the aggregated data profile for the Data Subject in the secure database(s). At this time, the DDID assigned to the attribute combinations may be re-assigned with respect to other actions, activities, processes or traits, or Data Subjects to continue obfuscation of data relationships, in one example.

[0179] Other implementations of the invention are contemplated herein, including various systems and devices. In one embodiment, disclosed herein is a system for improving electronic data security. In one example, the system may include an abstraction module configured to dynamically associate at least one attribute with at least one Data Subject; an abstraction module configured to generate DDIDs or accept or modify temporally unique, dynamically changing values to serve as DDIDs, and further configured to associate DDID with the at least one Data Subject; a maintenance module configured to track activity related to the DDIDs, and configured to associate any additional DDIDs, tracked activity, and time periods during which a DDID is used for conducting the tracked activity by means of time keys (TKs) or otherwise. In one example, the abstraction module is configured to add or delete attributes associated with the at least one Data Subject, and the abstraction module may be configured to modify attributes already associated with the at least one Data Subject.

[0180] In another implementation, disclosed herein is a device for conducting secure, private, anonymous activity over a network. In one example, the device may include a processor configured to execute program modules, wherein the program modules include at least a privacy client module; a memory connected to the processor; and a communication interface for receiving data over a network; wherein the privacy client that may reside on a Data Subject device, on a service provider device, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server is configured to receive TDRs including DDIDs and associated data attributes necessary for conducting

the activity over the network from a privacy server. In one example, the privacy client may be further configured to capture activity conducted using the device, and to relate the conducted activity to the TDRs. In another example, the privacy client may be configured to transmit the captured activity and TDRs to the privacy server. The privacy client may reside on a mobile device as a mobile application, in one example. The privacy client may reside in, and be accessible via, a network as a cloud based application, in another example. The privacy client may reside on the same computing device(s) on which the privacy server(s) resides as a local application, in another example.

[0181] In another example, the device may also include a geolocation module, wherein the TDRs are modified with information from the geolocation module, and wherein the TDRs restrict access to information regarding the identity of the device. The device may also include a user interface configured to allow a user to modify the TDRs, including options to change the DDID or data attributes associated with a particular TDR. The user interface may include selectable options for sharing the TDRs only with other network devices with a predetermined physical, virtual or logical proximity to the mobile device.

[0182] In another example, the device may receive, in response to TDRs, targeted advertising or marketing information based on the physical, virtual, or logical location of the device; wherein the TDRs include demographic information related to a user of the device, and further comprising receiving targeted advertising or marketing information based on demographic information. In another example, the TDRs may include information related to purchase transactions made or desired to be made using the device, and further comprising receiving targeted advertising or marketing information based on previous or desired purchase transactions.

[0183] In another implementation of the invention, disclosed herein is a system for providing electronic data privacy and anonymity. In one example, the system may include at least one user device having a first privacy client operating on the user device; at least one service provider device having a second privacy client operating on the service provider device; and at least one privacy server coupled to the network, the privacy server communicating with the first and second privacy clients; wherein the privacy server includes an abstraction module that electronically links Data Subjects to data attributes and attribute combinations and separates data into data attributes and attribute combinations, and the abstraction module associates a DDID with the data attributes and attribute combinations. In one example, the privacy server may include an authentication module that generates one or more of said DDIDs. In another example, the privacy server may include a maintenance module that stores a combination of the DDIDs with their associated data attributes and attribute combinations. In another example, the privacy server may include a verification module that verifies the integrity of data attributes, attribute combinations, and DDIDs. In another example, the privacy server may include an access log module that collects and stores information relating to the DDIDs and the data attributes for use in one or more post-incident forensic analysis in the event of an error. In one example, the DDID expires after a predetermined time, and after expiration of the DDID, the abstraction module assigns the DDID to another data attribute or Data Subject.

[0184] Figure 1B highlights some examples of how assignment, application, expiration and recycling of DDIDs may occur. It should be noted that, in the context of potential implementations of embodiments of the present invention, DDIDs may exist forever but be reused for multiple Data Subjects, data attributes, attribute combinations, actions, activities, processes and / or traits. While a DDID may be reused, two of the same DDIDs may not be used simultaneously unless so desired and authorized by the controlling entity. Reassignment of DDIDs may be accomplished by utilizing existing capabilities of data collection and analysis to reassign DDIDs to similar attribute combinations or Data Subjects, or to distinctly different attribute combinations or Data Subjects. This reassignment enhances the privacy / anonymity and security viability of the dynamically created and changeable digital DDIDs.

[0185] As indicated in Figure 1B, the system may be configured such that the assignment, expiration and / or recycling of any given DDID may occur based on any one or more of the following factors: (1) change in the purpose for which a DDID (and associated TDR) was created, e.g., association with a specific browsing sessions, Data Subject, transaction, or other purpose; (2) change in the physical location associated with a DDID (and associated TDR), e.g., upon exiting a physical location, upon arrival at a general physical location, upon arrival at a specific physical location, upon entering a physical location, or some other indicia of physical location; (3) change in the virtual location associated with a DDID (and associated TDR), e.g., upon entering a virtual location, upon changing a virtual location, upon exiting a virtual location, upon arrival at a specific page on a website, upon arrival at a specific website, or some other indicia of virtual location; and / or (4) based on temporal changes, e.g., at randomized times, at predetermined times, at designated intervals, or some other temporally based criteria. As may be appreciated, DDIDs separate data from context because, external to the system, there is no discernable relationship between Pertinent Data, the identity of a Data Subject or related party or Context Data associated with different DDIDs and / or TDRs. Internal to the system, relationship information is maintained for use as authorized by Data Subjects and trusted parties/proxies.

[0186] Figure 1C-1 represents the concept of a Circle of Trust (CoT) from the perspective of a trusted party or trusted proxy (indicated in Figure 1C-1 as "Trusted Proxy" and referred to herein as "Trusted Proxy" and / or "Trusted Party.") Note first that the Data Subject is included on the diagram at the bottom left. Diagrams of most current data use systems do not include Data Subjects since participation by Data Subjects generally takes the form of a binary decision whether to agree to "take-it-or-leave-it" online terms and conditions using the traditional "notice and consent" model. After that

initial point, the Data Subject typically loses all power to affect what happens to their data since "they are the product, not the customer." It is well acknowledged that this is a broken model for the digital age and provides few effective limitations on current or future use of data.

[0187] It should be noted that there may be more than one Trusted Party working cooperatively in connection with a single Circle of Trust and that Data Subjects may be participants in any number of Circles of Trust. Circles of Trust can be implemented by means of a centralized or federated model for increased security. Arrows in Figure 2 represent data movement; data inputs and outputs will contain different information.

[0188] Figure 1C-1 shows a data process flow for two potential embodiments of the invention. In a first example embodiment of the invention, a user (1) may indicate that they are interested in using the system to create data inputs regarding a specific Data Subject, (in this example, the user is the Data Subject) by forming one or more TDRs (each TDR may initially be comprised of a DDID intended to collect and retain data attributes associated with activity involving the TDR or comprised of a DDID together with data attributes or attribute combinations retrieved from the Data Subject's aggregated data profile) to participate, in this example embodiment, in the desired action of web browsing. Data associated with web browsing engaged in by the one or more TDR may be tracked and collected by the system and transmitted to a controlling entity serving as a trusted party or trusted proxy (3). The TDRs reflecting the tracked data collected in connection with the web browsing would represent output from web browsing which the controlling entity serving as a trusted party may select to augment the aggregated data profile of the user / Data Subject. In a second example embodiment of the invention, a user (2) may indicate that they are interested in using the system to create a privatized / anonymized version of a data set that the user has which contains personal information about Data Subjects (1). In this example, the data set of the user containing personal information about Data Subjects may serve as input to the system. The system may identify and track the data values contained in the data set reflecting personal information and the processing performed by the controlling entity serving as a trusted party or trusted proxy (3) may select said personal information to be replaced with DDIDs that require access to one or more Replacement Keys (RKs) to re-identify the personal information about Data Subjects. In this example, the resulting modified data set would represent output from the system containing dynamically changing DDIDs in lieu of personal information about Data Subjects. In this manner, the RKs could be altered in the future so that access to personal information about any one or more Data Subject may no longer be re-identified so the applicable Data Subject(s) have the "right to be forgotten," i.e., they can remove their digital traces from the Internet.

[0189] As shown in the boxes labeled "Privacy Policy" and "Authorization Request" in Figure 1C-1, data use may be managed by "Users" in accordance with permissions ("PERMs") managed by trusted parties and / or proxies. "Users" may be the Data Subjects themselves who are the subject of the data in question (e.g., users, consumers, patients, etc. with respect to their own data - for purposes hereof, "Subject Users"); and / or third parties who are not the subject of the data in question (e.g., vendors, merchants, healthcare providers, lawfully permitted governmental entities, etc. - for purposes hereof, "Non Subject Users").

[0190] PERMs relate to allowable operations such as what data can be used by whom, for what purpose, what time period, etc. PERMS may also specify desired anonymization levels such as when / where / how to use DDIDs in the context of providing anonymity for the identity and / or activities of a Data Subject, when to use other privacy-enhancing techniques in connection with, or in lieu of, DDIDs, when to provide identifying information to facilitate transactions, etc.

[0191] In a Data Subject implementation of the present invention (e.g., DRMI), Subject Users may establish customized PERMS for use of their data by means of pre-set policies (e.g., Gold / Silver / Bronze - note that this is only an example, and that mathematically, this could be a discrete set of k choices or it could be represented by a value on a continuum between a lower- and an upper-bound) that translate into fine-grained dynamic permissions or alternatively could select a "Custom" option to specify more detailed dynamic parameters.

[0192] In a "stewardship" implementation of Dynamic Anonymity (DRMD), Non Subject Users may establish PERMs that enable data use / access in compliance with applicable corporate, legislative and / or regulatory data use / privacy / anonymity requirements.

[0193] Within the CoT reflected in Figure 1C-1 based on PERMS, business intelligence, data analysis and other processes may be performed by means of any combination or interpolation of I, D, T and / or X with regard to one or more Data Subjects, as shown in TABLE 3 below:

TABLE 3

"I"	"D"	"T"	"X"
Identifier for Data Subject	Value of Assigned Dynamic De-Identifier	Time period of association between I and D	Pertinent Data during T

[0194] Figure 1C-2 shows a Circle of Trust (CoT) from a Data Subject perspective.

[0195] Figure ID illustrates a smartphone application that can track both geolocation and blood pressure levels. Using

Dynamic Anonymity, such a device could split data into two streams, each obscured such that either stream, if intercepted and / or compromised (or even examined once stored), would not reveal Personal Data (PD) without the addition of critical information protected within the CoT.

[0196] More particularly, Figure ID illustrates:

1. The blood pressure monitoring application (A) contacts a Trusted Party within a Circle of Trust (B) requesting a DDID for the Data Subject patient.
2. The CoT Trusted Party provides a DDID for the Data Subject.
3. An application operated by the Trusted Party sends back two sets of periodically-changing information (one for GPS data, one for blood pressure levels), each consisting of DDIDs, offsets (to obscure blood pressure level data and geographic position), and encryption keys; refreshed for each new time period. (These are also stored to a database for later use.)
4. The monitor application transmits two encrypted and obscured streams of data to a Dynamic Anonymity-controlled "proxy" application or network appliance (C) within its corporate network. (Here, both location and levels have a periodically changing offset applied to them.)
5. The "proxy" (C) uses the streams of data (D & E) from the Trusted Party (containing only decryption keys) to convert the transmitted data into "plaintext." The proxy also hides the incoming IP address and provides stream(s) (containing multiple Data Subjects' information) of DDIDs and obscured blood pressure level data (F) or GPS locations (G) to the corresponding databases (H) and (I).

[0197] At each point in Figure ID outside of the Circle of Trust (and outside the smartphone itself) the patient's data is protected; no Personal Data (PD) is made available or ever produced.

- Transmissions to and from the Trusted Party (1, 2) have no privacy / anonymity -harming Personal Data, nor is any stored in the Trusted Party's database.
- Location and blood pressure levels (4) are transmitted separately (intercepting any one stream reveals nothing), keyed by DDIDs, and obscured so that even the data itself neither reveals nor contains anything, directly or indirectly, about the patient's true location or blood pressure levels.
- The Dynamic Anonymity proxies (C) must be connected to the Trusted Party in order to decrypt the data (preventing a man-in-the-middle attack). Each merges multiple streams of data together, after decryption, so that the originating IP address cannot be associated with its decrypted data.
- Once at rest, when residing in two separate databases (H and I), the blood pressure levels and location data each have different sets of DDIDs, so that even the hosting company cannot draw any association between the two, much less link each set of data to the Data Subject who produced it.

[0198] Figure IE illustrates use of one embodiment of the invention to assist in the task of choosing a location for a new clinic to serve patients who are 20 to 30 years old with sexually transmitted diseases (STDs). One "cleansed" data set may show the incidence of STDs, aggregated by neighborhood to protect privacy / anonymity. Another data set may show how many patients reside in each neighborhood. But, even when these are aggregated, one cannot know exactly how many identified cases of STDs fall into particular age ranges.

[0199] Dynamic Anonymity alleviates this dilemma by supporting two different modes of analysis.

[0200] In cases where data must be exposed externally (that is, outside the CoT), Personal Data elements can be obscured or encoded as DDIDs, with the resulting associations stored inside the CoT. Additionally, when required, the data (or field) type identifiers can also be obscured in a similar manner.

[0201] Later, after analysis is performed, the results of that analysis can then (when permitted) be associated back with the original Data Subjects, field types, and values.

[0202] Another way Dynamic Anonymity enables lossless analysis is through the use of federated, anonymized queries, either among different Trusted Parties within a CoT, different data stores within the same Trusted Party, or between Trusted Parties and application developers whose data stores reside outside the CoT.

[0203] Consider again the problem of choosing where to site a clinic to serve patients who are between 20 and 30 years old with STDs. The Dynamic Anonymity system improves upon existing techniques by allowing the target query to span multiple data stores and dividing it up such that each participant does not know what purpose it serves, so there is no risk of divulging PD.

[0204] In this scenario, the query for the number of patients who are 20 - 30 years old with STDs within a set of (sufficiently large) geographic areas is presented to numerous Trusted Parties within the Circle of Trust. This aggregate query is then broken down into several steps, such as:

1. Find patients between 20 - 30 years of age in some broad geographic area.

2. Select only those with STDs.
3. Select only those whose privacy / anonymity policies allow this level of analysis.
4. "Join" those results to the home addresses of those patients.
5. Aggregate these results by neighborhood, revealing only counts of patients.

[0205] The actions needed to satisfy this query could span completely different data stores, in different organizations - nonetheless protected and facilitated by the Circle of Trust.

[0206] Figure IE shows the following processes:

1. The prospective clinic owners send a query to a Trusted Party, asking to find individuals who are between 20 - 30 years old with STDs.
2. The Trusted Party contacts healthcare-related data stores to find individuals who are between 20 - 30 years old with STDs.
3. The healthcare-related data stores (which store diagnoses by DDIDs rather than by identifiable keys) find matching records.
4. Matching DDIDs are then transmitted back to the Trusted Party.
5. The Trusted Party then resolves these DDIDs to unveil identified individuals.
6. The Trusted Party filters that list by those whose privacy / anonymity policies allow this particular kind of query.
7. The CoT then uses a database of their addresses to aggregate counts (or incidence frequency, if the query is incomplete) by neighborhood, producing the desired result.

[0207] In this scenario, companies operating healthcare-related databases do not need to know (or divulge) the identity, location, or other potentially identifiable information of the patients whose data they possess. The records they possess are keyed by DDID, and also potentially obscured, so that no Personal Data is generated when performing the specified query, nor when transmitting results.

[0208] Note that the party posing the query does not have access to this information. Their only interaction with the CoT consists of posing a question and receiving a high-level, aggregated, non-PD result. Note that not having access to this information in no way affects the quality, accuracy or precision of the end result. Dynamic Anonymity thus eliminates Personal Data that contributes nothing to the end result and that only serves to weaken privacy / anonymity without any attendant benefit to any other party. By filtering out irrelevant data, the analysis of which would otherwise consume time and resources, Dynamic Anonymity actually *increases* the utility and value of the information received.

[0209] Personal Data is only produced temporarily, *within the Circle of Trust* managed by the Trusted Party (the appropriate place for such information) - such as when the DDIDs are resolved. Such operations are *transient* and leave no lasting trace other than the intended query result, and could also be confined to certain dedicated servers for increased security. The use of DDIDs in the context of Circles of Trust avoids potential shortcomings of normal data analytics that could generate discriminatory or even identifiable results.

[0210] Figure IF illustrates use of one embodiment of the present invention to enable a shoe manufacturer to send a coupon for a new line of shoes to people who have recently performed web searches related to the sport of running within a certain city. In exchange for offering discounts on the shoes, the manufacturer wishes to receive qualified consumers' email and / or home addresses, and to send those who redeem the coupon a survey to assess their satisfaction with the new shoe.

[0211] Explanation:

1. The manufacturer, outside the CoT, purchases a list of matching DDIDs from a search engine.
2. The DDIDs are submitted to one or more Trusted Parties, accompanied by an offer letter and a policy modification allowing access (upon acceptance) to Data Subjects' email and / or home addresses.
3. Each Trusted Party then forwards the offer letter to the Data Subjects matching those DDIDs (provided they have opted-in to receiving such an offer).
4. If a Data Subject recipient accepts the offer, the recipient's policy is updated with (perhaps temporally-limited) permission for exposing their home and/or e-mail addresses to the shoe company.
5. The shoe manufacturer, now part of the CoT, but only with respect to this specific offer and only in the most limited sense, then receives a list of e-mail and home addresses of those who wish to receive the coupons. Note that this list is necessarily highly targeted and accurate and therefore of maximum value to the shoe manufacturer. This is precisely how the CoT, by increasing privacy / anonymity, also increases value. The shoe manufacturer may be assured that all mailings done this way will be sent to those with substantial interest in the manufacturers' offer.

[0212] Figure 1G builds upon the prior example in Figure ID where a GPS-enabled blood pressure monitor securely stored patients' locations and blood pressure levels via Dynamic Anonymity. Dynamic Anonymity may be leveraged to:

1. Avoid imposition of HIPAA data handling obligations on business associates involved in data processing flows if data in their possession does not constitute Personal Data (PD).
2. Ensure that access to, and use of the data, by the physician satisfies HIPAA obligations.

[0213] Note that the following scenario assumes that both a Data Subject patient and his / her physician have accounts inside the Circle of Trust.

Explanation:

[0214]

1. The monitoring application cooperates with the patient's Trusted Party to allow the patient to update his / her privacy / anonymity policy rules so that his / her physician can now access his / her blood pressure levels (but not his / her GPS location data). Note that this grant can be temporary (analogous to the temporally limited nature of photographs that can be shared with Snapchat - the grant expires after a period of time) - or ongoing.
2. The physician (via his / her web browser) browses to the blood pressure monitor's web site, which launches a JavaScript-based blood pressure level viewer application which thus *runs in the physician's browser,* and not on the monitor company's servers (i.e., that the stitching together of data necessary to make it personally identifiable is done via the Trusted Party server which is itself trusted - see steps 4 and 5 below).
3. The blood pressure-level viewing application asks the physician to log in via her Trusted Party (similar to the way many applications allow you to authenticate using a FACEBOOK® or GOOGLE® account), and receives a session cookie that continues to identify them to that party. (FACEBOOK® is a trademark of Facebook, Inc.)
4. After the physician selects a range of time to view, the viewer application requests the relevant DDIDs and offsets from the Trusted Party, for that patient.
5. The Trusted Party validates the physician's access to this information (checking the patient's privacy / anonymity policy rules) and then returns the DDIDs and offsets.
6. The viewer application then contacts its own corporate website, requests the blood pressure data corresponding to those DDIDs, receives the result, applies the offsets, and renders the blood pressure levels as a graph.

[0215] At this point, the image on the physician's screen is HIPAA-protected PHI data. If the physician prints the data, that paper will be subject to HIPAA. When the physician is done viewing the graph, he / she logs out or closes the browser, the application ends, and the data is erased.

[0216] Note that re-identified HIPAA-controlled data only resides in the physician's browser. The original blood pressure level data stored in the application provider's databases remains untouched and obscured. The Trusted Party's data remains unaffected as well.

[0217] Also note that the permission to view the blood pressure data is enforced within the Circle of Trust. It is not enforced (as is common practice today) merely by the viewer application - or only by the application's backend servers. This means that an adversary could not gain unauthorized access to the data merely by hacking into the blood pressure level viewer application, because the data would not be there in any usable or identifiable form. The dynamic data obscuring capabilities of Dynamic Anonymity DDIDs combined with the dynamic data privacy / anonymity control capabilities of a "Circle of Trust," maximize both data privacy / anonymity and value to support personalized medicine / medical research.

[0218] With respect to Figure 1H, the different nodes depicted in 1H-A represent data elements related to two different Data Subjects that are capable of being tracked, profiled and / or analyzed by third parties because they can be associated with, and / or re-identified for, each of the Data Subjects. 1H-B represents a simplified visual depiction of the same data elements that can be retained with Dynamic Anonymity without loss of context. The Family Educational Rights and Privacy Act (FERPA) is a federal privacy statute that regulates access to and disclosure of a student's educational records that disclose personally identifiable information (PII). FERPA provides that PII cannot be disclosed, however, if PII is removed from a record, then the student becomes anonymous, privacy is protected, and the resulting de-identified data can be disclosed. In addition to statutorily defined categories (e.g., name, address, social security number, mother's maiden name, etc.), FERPA defines PII to also include "...other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty." The ability of Dynamic Anonymity to obfuscate connections between each of the Data Subjects and the data elements in a controlled manner by means of an Anonos-enabled Circle of Trust (CoT), as visually depicted in 1H-B, enables educational-related data to be used without disclosing PII.

[0219] Figure 1I shows an example of a process to perform Disassociation Level Determination (DLD) and create an Anonymity Measurement Score (AMS), in accordance with one embodiment of the invention. Determining DLDs may

entail undertaking a mathematical and / or empirical analysis of the uniqueness of a data element prior to Disassociation to assess the level of Disassociation required to reduce the probability of identification or re-association by adversaries without proper permission. DLD values may be used as input to determine the relevant level of Disassociation/Replacement appropriate for different types of data elements.

[0220] AMS may be used to correlate mathematically derived levels of certainty pertaining to the likelihood that personally sensitive and / or identifying information may be discernible by third parties to tiered levels and / or categories of anonymity. In other words, AMS values may be used to evaluate the output from Disassociation/Replacement activities to determine the level/type of consent required before data can be used.

[0221] In Step (1) of Figure 1I, data attributes may be evaluated to assess DLDs, i.e., data elements are analyzed to determine the potential likelihood of directly or indirectly revealing personal, sensitive, identifying or other information with regard to which anonymity protection is desired. In Step (2), based at least in part on the determined DLDs, the data elements may be dynamically anonymized by means of Disassociation. In addition, data elements may also undergo Replacement. In Step (3), a calculation may be performed, e.g., by means of a mathematical function/algorithm (e.g., the mathematical function / algorithm whose output is reflected in Figure 1J) to calculate an AMS that correlates to the likelihood that the identity of the Data Subject to which said data attributes pertain may be discernible by third parties after Disassociation/Replacement with DDIDs. Finally, in Step (4), the score/rating calculated in Step (3) above may be used to specify the level of consent/involvement required by the Data Subject to which the anonymized data attributes pertain versus what level of discretion/use a third party may exercise with regard to the anonymized data attributes without requiring consent/involvement by the Data Subject, such as is shown in the example AMS usage reflected in Figure 1K below.

[0222] Different categories of information hold different statistical likelihoods of being re-identifiable. Every data element has associated with it with an inherent level of uniqueness as well as a level of uniqueness when combined with other pieces of data as determined by placement, order and / or frequency of occurrence. For instance looking at single data points, a social security number is highly unique and therefore more easily re-identifiable than a single data point such as sex, since each person has an approximate 1:1 probability of being male or female. Since gender is less unique as an identifier than a social security number, gender is significantly less likely on an independent basis to re-identify someone than a social security number.

[0223] The Anonymity Measurement Score (AMS) measurement schema ties statistical probabilities of re-identification to create multiple ratings depending on the level and degree of disassociation and / or replacement applied to data elements. As a single data point example, a social security number, which has not been disassociated or replaced at all, may merit an AMS rating of 100 meaning the uniqueness classifies it as a very high risk of re-identification. Whereas sex as a single data point identifier without disassociation or replacement may merit an AMS score of 10 since it is classified at a low risk of re-identification even without de-identification measures in place.

[0224] In an example implementation with a social security number as a singular data point, a Level 1 implementation could assign DDIDs for purposes of disassociation and / or replacement while retaining the initially assigned value - i.e. permanent assignment (e.g., where data is used as output in hard copy representations of the data). In the case of a social security number, a Level 1 application of DDIDs could reduce the AMS score by 10% and result in a modified AMS score of 90. This is still a high level of risk associated with re-identification but is more secure than non-disassociated and / or replaced elements.

[0225] In an example Level 2 implementation, the social security number could have DDIDs assigned for purposes of disassociation and / or replacement while retaining the initially assigned value until the value is changed on a one-directional basis - i.e. ad hoc changeability (e.g., where data values can be changed unilaterally by sending new information to remote cards, mobile, wearable and / or other portable devices that include means of electronically receiving and storing information). The social security number AMS score could thereby be reduced another 10% to achieve an AMS score of AMS.

[0226] In this example, continuing to a Level 3 implementation, it could have DDIDs assigned for purposes of disassociation and / or replacement whiled retaining the initially assigned value but the DDIDs could change on a bidirectional basis, i.e. dynamic changeability (e.g., where data values can be changed bilaterally by sending and / or receiving data dynamically between client / server and / or cloud / enterprise devices with the ability to receive and change specified data dynamically). The social security number would then have an AMS score that is further reduced by 50% resulting in an AMS score of 40.5.

[0227] As de-identification measures are applied to a data point through disassociation and / or replacement via use of DDIDs, the risk of re-identification is lowered. AMS score determinations are derived from the function of the likelihood of an identifier or identifiers taken together to be re-identifiable. This, combined with the processes used to obfuscate data elements can then be separated into categorical or other types of classification schemas to determine various functions such as permitted uses and what level of permission entities need to have before using data. This process may also be applied to single or aggregated AMS scores. Aggregated AMS scores are the likelihood of multi data point re-identification expressed through AMS scores as compounded together to express the level of uniqueness of combined

data points.

[0228] As an example of a possible categorical classification schema, the AMS score could be broken into Categories A, B and C. Where category A is data with a single or aggregated score of 75 or more may be used only with current, express and unambiguous consent of the Data Subject. Category B may represent a single or aggregated AMS score of 40 to 74.9 that would mean the data set could be used with (i) current or (ii) prior express consent of the Data Subject. A Category C could represent a single or aggregated AMS score of 39.9 or lower which could allow for use of the data set without requiring consent of the Data Subject.

[0229] In the example disclosed in Figure 1J, each of the identifiers other than the Social Security Number discussed above (i.e., Credit Card Number, First Name, Last Name, Birthdate, Age and Sex) are similarly assigned a Non-Disassociated / Replaced AMS rating in the first column. In each of the next two subsequent columns (i.e., Level 1 and Level 2) their AMS scores are adjusted by successive 10% reductions, and in the last columns (i.e., Level 3) their AMS scores are adjusted by a 50% reduction, resulting in decreasing AMS scores as DDID-enabled obfuscation increases by means of permanent assignment (Level 1), ad hoc changeability (Level 2) and dynamic changeability (Level 3).

[0230] As mentioned above, Figure 1J illustrates exemplary calculated Anonymity Measurement Scores, in accordance with one embodiment of the invention. These AMSs are for illustration purposes only and demonstrate the fact that certain types of potentially personally-identifying information is more likely to reveal a Data Subject's true identity than other types of information, and that additional levels of Disassociation/Replacement, e.g., ad hoc (i.e., Level 2) and / or variable changeability (i.e., Level 3), may increase the amount of anonymity afforded to the Data Subject by the anonymization systems and scheme.

[0231] As mentioned above, Figure 1K illustrates exemplary categories for the level of consent/involvement required by the Data Subject for certain calculated Anonymity Measurement Scores, in accordance with one embodiment of the invention. These categorizations are given for illustration purposes only and demonstrate the fact that certain aggregated scores may apply different categories of treatment. For example, Category A data may be used only with current, express, and unambiguous consent of the Data Subject; while Category B data may be used with current or prior express consent of the Data Subject; and Category C data may be used without requiring consent of the Data Subject. Other schemes may be employed to meet the needs of a particular implementation.

[0232] Figure 1L shows an example embodiment of the present invention using DDIDs for emergency response purposes. In Step (1) of Figure 1L, data attributes are evaluated to determine applicable emergency response distinctions - e.g., whether a house is located in a flood plain, whether an individual is in immobile or in need of particular life saving equipment or medical care. In Step (2), applicable data elements are dynamically anonymized by a trusted party by means of disassociation and / or replacement using DDIDs to protect the privacy / anonymity of citizens and the obfuscated information is sent to a DDID-obfuscated emergency response database. In Step (3), information is evaluated by the trusted party to determine data elements relevant to respond to a specific emergency. Finally, in Step (4), the trusted party provides to the obfuscated emergency response database association keys (AKs) and / or replacement keys (RKs) necessary to reveal desired information otherwise represented by DDIDs for the duration of the emergency event and associated response.

[0233] In the example embodiment reflected in Figure 1L, data is resident in an emergency response database in a dynamic DDID obfuscated state such that identifying information is not discernable or re-identifiable until such time as necessary association keys (AKs) and / or replacement keys (RKs) are provided when an appropriate triggering incident occurs. A triggering operation carried out by a trusted party would issue time sensitive AKs / RKs with respect to portions of appropriate data at specified levels of obfuscation or transparency depending on the type of incident. Identifying information could be maintained inside the emergency response database but in a dynamic DDID obfuscated state; a data mapping engine controlled by a trusted party would maintain correlative information pertaining to dynamically changing DDIDs and AKs / RKs necessary to discern and / or re-identify data which would only be provided upon the event of an appropriate emergency incident.

[0234] Policy external to the system would determine which information may be relevant for different incidents and stages of incidents, as well as what level of obfuscation / transparency is appropriate at different times so not all information would released at once and so that irrelevant but sensitive information would not released without cause. These permissions would then be encoded for ease of triggering access in an emergency. This method allows for bidirectional communication with, and verification of the locations of, impacted individuals compare to capabilities of static lists or unidirectional communication.

[0235] AKs / RKs would be changed and reintroduced to the emergency response database after each incident so that information would be maintained on an ongoing electronic basis in a DDID obfuscated state, i.e., a new trigger would be required to make portions of data readable via new AKs / RKs following a prior release of AKs / RKs in response to an earlier incident (i.e., following resolution of an emergency response incident, AKs / RKs previously provided would no longer reveal the underlying identifying information associated with dynamically changing DDIDs. This would protect the privacy / anonymity of individual citizens while protecting their safety in major incidents by allowing appropriate access to data for a limited period of time. On the emergency management side, this could reduce the need for resource

intensive information intake and handling procedures employed during large incidents.

[0236] Additionally, new data pertaining to individuals could be added during incidents, such as 'accounted for' or 'missing' status designation during evacuation. This new input could become part of an individual's personal profile held in stasis by an embodiment of the present invention and maintained for future authorized use if helpful in the same, or subsequent emergency.

[0237] In a local opt-in example, citizens could register to have information that would be relevant in an emergency stored in a DDID obfuscated emergency database. The emergency database could be stored locally or elsewhere but could be interoperable in case of cross-jurisdictional incidents. Once the citizen data is input into the DDID obfuscated system, no one could see or access the data in a discernable or re-identifiable manner until a trigger mechanism controlled by a trusted party results in release of dynamic, situational based AKs / RKs as necessary to discern / re-identify appropriate components of the stored data.

[0238] Two examples of emergency management views of potential embodiments of the present invention could include:

1. Interactive screen(s) could present overlays that allow Geographic Information System (GIS) and other data to be imposed or correlated to location specific data - i.e. clicking on a house may show information that has been submitted by a citizen as well as information that a jurisdictional authority has on the subject property as well as associated disaster risks. For instance, flood alerts are a great example of a notification that could provide different amounts of information on different people depending on their specific location. A general flood warning may go out to an entire area but a specifically targeted warning may be sent to those directly in the flood plain who are at greater risk for flooding.
2. More traditional formats, such as electronic tables, etc. could be augmented to provide non-geographic data.

[0239] The above two variations in format could be interoperable as well with the data from each being represented in the other either interactively or linked.

[0240] In the case of watches and warnings, the locality of the weather phenomenon (as determined via weather radars, GIS mapping, etc.) will determine the subset of information released, which may be further revealed inside the database.

[0241] In another example case, there may be a criminal who is profiling a particular demographic as targets. In this situation, DDIDs such as contact and demographic information would be relevant-in addition to partially obfuscated location data-in order to create general perimeters on the message send out. The relevant data fields and their DDIDs would be activated to point to individuals matching the demographic, who may then be put on notice of the criminal activity.

[0242] In an emergency situation that requires evacuation, this information could be triggered to assist emergency personnel in more effective resource deployment in addition to assisting in evacuation or identifying those who may need additional assistance in emergency situations. In another example, such as a blizzard, the system could be triggered to let emergency personnel know exactly where kidney dialysis patients are located in their city for emergency transportation via snowplow by means of GPS location information associated with mobile devices associated with the patients - which information would be represented by indiscernible / non re-identifiable DDIDs until such time as a trigger event results in the release applicable AKs/ RKs reflecting appropriate correlative information.

[0243] Figure 2 shows an example of process operations or steps that may be taken by the abstraction module of the privacy server, in accordance with one embodiment of the present invention. In one example, at step 1 a related party ZZ (shown as "RP ZZ") sends a request via a privacy client that may reside on a Data Subject device, on a service provider device, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server to the privacy server with respect to a desired action, activity, process or trait. The request initiation may be configurable so that it is predictable, random, automatically or manually initiated. For instance, related party RP ZZ initiates a request for a desired online action of web browsing.

[0244] At step 2, in one example the abstraction module of the privacy server determines the attribute combinations necessary to perform with respect to a desired action, activity, process or trait and retrieves them from the database as attribute combination A ("AC A"). In this example implementation of the system, the abstraction module of the privacy server is configured to add or delete attributes, retrieve attribute combinations, and to modify attributes within any given combination.

[0245] In an example involving an ecommerce site selling sports equipment, the abstraction module of the privacy server may determine that attributes pertaining to a Data Subject's height, weight and budget are necessary to perform with respect to a desired action, activity, process or trait and therefore may retrieve the attributes of height, weight and budget for the specified Data Subject from the database to form an attribute combination comprised thereof. In another example involving a physician requesting blood pressure information, the abstraction module of the privacy server may determine that attributes comprised of the most recently recorded systolic and diastolic blood pressure values are necessary to perform with respect to a desired action, activity, process or trait and therefore may retrieve the most

recently recorded systolic and diastolic blood pressure values for the specified Data Subject to form an attribute combination comprised thereof. Another example may involve an Internet user that goes to an online retailer of running shoes. The online retailer may not know who the user is or even if the user has visited the site one or more times in the past. The user may want the visited site to know he has been shopping for running shoes and may want the visited site to know what shoes the user has looked at over the last few weeks on other sites. The user may notify the privacy server to release only the recent shopping and other user defined information to the visited site. As a result in this example, the privacy server may select the following attributes: shoe size = 9, shoes recently viewed at other websites = Nike X, Asics Y, New Balance Z, average price of the shoes viewed = $109, zip code of the shopper = 80302, gender of the shopper = male, weight of the shopper = 185 lbs. The privacy server may collect these attributes, generate a unique DDID or accept or modify a temporally unique, dynamically changing value to serve as the DDID and assign the DDID to the attributes and send the same to the visited website as a TDR. If the user views a Saucony model 123, the website may append this attribute to the information pertaining to the attributes related to shoes viewed and send this information back to the privacy server as part of the augmented TDR.

[0246] Yet another example may involve a personal banker at a bank who is working with a client who wants to add a savings account to the accounts she otherwise holds with the bank. The personal banker may not need to know all information about the client, just the information necessary to open up the account. Using the present invention the banker may query the bank's privacy server via a privacy client to request opening up a new savings account for the customer. The bank's privacy server may determine the data authorization limits for the requester and for the desired action. The bank's privacy server may collect the following attributes on the customer: name = Jane Doe, current account number = 12345678, type of current account = checking, address of the customer = 123 Main Street, Boulder, CO 80302, other signatories on the checking account = Bill Doe, relationship of signatory to customer = husband. After the bank's privacy server collects these attributes, it assigns a DDID for these attributes and sends the information to the personal banker via a privacy client as an augmented TDR.

[0247] The controlling entity could elect, in one example, to include data attributes in attribute combination A that enable recipients of the TDR to use existing tracking technology to track related party ZZ anonymously for the duration of existence of the resulting TDR. The controlling entity may also elect to include data that is more accurate than that available via existing tracking technologies to facilitate personalization and customization of offerings for related party ZZ.

[0248] At step 3, in one example, a request is made of the privacy server ("PS") for a DDID. This may include a request for specified levels of abstraction, and for the generation of a unique DDID or acceptance or modification of a temporally unique, dynamically changing value to serve as the DDID to be used in the system corresponding with respect to a particular activity, action, process or trait requested. Before assigning the DDID, the PS may verify that the DDID value is not actively being used by another TDR, potentially including a buffer period to address potential outages and system down time.

[0249] At step 4, in one example the abstraction module of the PS assigns and stores the DDID in response to requests with respect to actions, activities, processes or traits. Step 4 may also include in one example the operation of assigning a DDID X for the web browsing requested by related party ZZ.

[0250] At step 5, in one example the abstraction module of the PS combines the retrieved applicable attribute combination and assigns DDID X to create the TDR. The TDR itself may not include information about the real identify of related party ZZ, but the maintenance module of the privacy server may retain information necessary to re-associate the TDR with related party ZZ. Operation 5 may also include the secure database(s) associating the attribute combination request with the Data Subject associated with the attribute combination, thereby providing an internal record in the aggregated data profile for the Data Subject associating related party ZZ with particular attribute combination A that are deemed necessary to perform with respect to a desired action, activity, process or trait.

[0251] Figure 3 shows examples of additional steps that may be taken by the abstraction module of the privacy server, in accordance with one embodiment of the present invention. At step 6, in one example the TDR created for related party ZZ's web browsing request is transmitted via the privacy client that may reside on a Data Subject device, on a service provider device, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server to the applicable service provider, vendor, or merchant. The privacy client may also capture data associated with the desired browsing activity with the service provider, vendor or merchant.

[0252] Once the TDR's purpose is served or a predetermined temporal limitation is reached, in one example the TDR may be sent via the privacy client back to the privacy server, at step 7, the TDR that comes back may be augmented with new attribute combinations with respect to a desired action, activity, process or trait for which the TDR was created. In the example shown in Figure 3, related party ZZ performs the desired web browsing in connection with the service provider, merchant or vendor, and attribute combination Q ("AC Q") is generated that reflects attribute combinations associated with the desired web browsing performed. When the web browsing is complete, or when the temporal limitations of the TDR expire, the privacy client with the TDR, now augmented with attribute combination Q reflecting data associated with the web browsing, transmits data from the service provider, vendor or merchant to the privacy server. When the data is received back at the privacy server, a time period/stamp is associated with the TDR in one example

by means of time keys (TKs) or otherwise, and the relevant attribute combinations returned from the service provider, vendor, or merchant may be updated and stored in the secure database(s) in the aggregated data profile for the Data Subject.

[0253] Figure 4 shows an example of additional steps that may be taken following the operations of Figure 3, according to one example of an embodiment of the present invention. As each augmented TDR is received back by the privacy server, the maintenance module of the privacy server may update the source data by associating the time period/stamp by means of time keys (TKs) or otherwise, DDID, and attribute combinations with the applicable Data Subject. As shown in the example of Figure 4, the privacy server may record and associate the time period/stamp by means of time keys (TKs) or otherwise, DDID, attribute combination A, and attribute combination Q with requesting related party ZZ within the secure database. Relationship information between and among time periods/stamps, DDIDs, attribute combinations, Data Subjects and associated profiles may be stored, updated or deleted as applicable in the maintenance module of the privacy server. This may include, in one example, storing or updating all relationship information between all time periods/stamps, DDIDs, attribute combinations, Data Subjects, and profiles within the secure database(s) in the aggregated data profile for the Data Subject. Upon completion of the association of new data with regard to the desired action, activity, process or trait from the attribute combinations, in one example the DDID may then be reassigned for use with new TDRs in the same fashion as described above.

[0254] Figure 5 highlights differences between an example single layer abstraction implementation of a system, as compared to an example multi-layer abstraction implementation of a system, in accordance with one embodiment of the present invention. Example 1 illustrated in Figure 5 shows an example of a system with a single layer of abstraction, such as described above in the discussion of Figures 2-4 with respect to a web browsing activity. Example 1 in Figure 5 shows an example of a final disposition resulting from the web browsing activity of Figures 2-4, where the secure database is updated with a record associating a time period/stamp by means of time keys (TKs) or otherwise, attribute combination A, attribute combination Q, and DDID X associated with requesting related party ZZ. It should be noted that with respect to Example 1, parties outside of the system would not have access to identifying information pertaining to attribute combinations or Data Subjects. However, within the system, though the user of a replacement key (RK) described herein, the identity of related party ZZ would be discernible in one example, as would the relationship between related party ZZ, attribute combination A, attribute combination Q, the time period/stamp and DDID X.

[0255] Example 2 in Figure 5 reflects one potential implementation of a multi-layer abstraction implementation of a system, in accordance with one embodiment of the present invention. The abstraction provided is a function of multiple applications of the system, rather than of wholly different pieces. The dynamic nature of the TDRs allows for the same baseline principles to be used among the levels of abstraction while still providing useable interaction with regard to data as requested. In this example, an entity with authorized access to privacy server A and associated secure database would have access to the associations between DDID X, DDID P, DDID TS and DDID YY, as well as each of the attribute combinations and time periods/stamps associated with the DDIDs. However, the entity would not have access in one example to any information concerning associations between the different DDIDs disclosed. Only upon gaining access to privacy server B and associated secure database would the second level of abstraction be revealed pertaining to the relationship between DDID X and DDID and between DDID TS and DDID YY. As shown in Figure 5, this second level of abstraction could be the relationship of Subject DD to DDIDs X and P, and the relationship of Subject CV to DDIDs TS and YY.

[0256] In the event that Subject CV and Subject DD reflect the identity of Data Subjects in question, Example 2 would reflect one potential implementation of a two-layer abstraction implementation of the system. However, if the values for Subject CV and Subject DD were each assigned dynamically changeable DDIDs, then Example 2 would reflect one potential implementation of a three-layer abstraction implementation of the system. It should be appreciated that any and all of the elements of the system can be abstracted on multiple levels in order to achieve desired levels of security and privacy / anonymity.

[0257] In one example implementation of the system, both Example 1 and Example 2 in Figure 5 may represent an authenticated data structure that permits the verification module of the privacy server to validate and verify attribute combinations and DDIDs embodied in a TDR and / or data profile at any point in time by methodologies such as cyclic redundancy checks ("CRCs"), message authentication codes, digital watermarking and linking-based time-stamping methodologies. These methodologies enable verification of the state and composition of data at various points of time by confirming the composition of each Data Subject, attribute, attribute combination, aggregated data profile and other elements contained in the privacy server at different points in time.

[0258] In addition, in one example implementation of an embodiment of the present invention, both Example 1 and Example 2 in Figure 5 may include data necessary for the access log module to enable post-incident forensic analysis in the event of system related errors or misuse.

[0259] Figure 6 shows one example of a process for providing data security and data privacy / anonymity, in accordance with one embodiment of the present invention. Figure 6 shows process steps that may be implemented by a controlling party or a system, in one example. The operations outlined in Figures 6 - 10 may be facilitated by means of known

programming techniques including but not limited to Simple Object Access Protocol (SOAP), Representational State Transfer (REST) Application Programming Interfaces (APIs) or Service Oriented Architecture (SOA) techniques as well as canonical industry standard data models such as HL7 for healthcare, SID for telecom, ARTS for retail, ACORD for insurance, M3 for multi-commodity models, OAGIS for manufacturing and supply chains; PPDM for oil & gas/utilities, and the like.

[0260] At step 1 in Figure 6, a data attribute is received or created as input to the system. As noted previously for purposes of this disclosure, a data attribute refers to any data element that can be used, independently or in combination with other data elements, to identify a Data Subject, such as a person, place or thing, or associated actions, activities, processes or traits. One example of a data attribute may be the street address comprised of 1777 6th Street, Boulder, Colorado 80302.

[0261] At step 2 of Figure 6, the data attribute is associated with the applicable subject. In the above example, the data attribute address is associated with the subject Colorado Municipal Court Building.

[0262] At step 3 of Figure 6, the elements associated with each data attribute are linked to or binded with the data attribute and determinations are made comprising applicable category(s); value(s) and classification(s) pertaining to attributes to facilitate use of the attributes with respect to desired actions, activities, processes or traits. For example, elements associated with the above data attribute address may be: (a) categorized as a street address; (b) with values of: 1; 7; 7; 7; 6th; S; t; r; e; e; t; B; o; u; 1; d; e; r; C; o; 1; o; r; a; d; o; 8; 0; 3; 0; 2; 1777; 6th Street; Boulder; Colorado; 80302 or any combination of the foregoing; and (c) classified as constant in nature since the building is stationary. Another example of a data attribute pertaining to the subject building may be the condition of the building (a) categorized as the condition of the building; (b) with a value of good condition; and (c) classified as variable in nature since the condition of the building may improve of degenerate over time. Another example of a data attribute pertaining to the subject building may be (a) categorized as organizations having offices located in the building; (b) with a value of Boulder Colorado Alternative Sentencing Program (CASP); and (c) classified as variable in nature since CASP may in the future change the location of their office. It should be noted that exogenous information may comprise attributes associated with a Data Subject. For example, in the case of the building identified above, if someone knows that Boulder Colorado Alternative Sentencing Program (CASP) has offices at the Colorado Municipal Court Building and discovers that John Smith works at CASP and that on weekdays John Smith shows up at 1777 6th Street in Boulder, that original person may use this exogenous information to discern the address of the Colorado Municipal Court Building in Boulder. Thus the fact that John Smith works at CASP may be an attribute of the Data Subject, potentially revealing the Data Subject, i.e., the building at the address.

[0263] At step 4 in Figure 6, each of the data attributes input into the system are added to an aggregated data profile (see, e.g., Figures 1 and 1A) for the Data Subject. In the above example, the noted data attributes would be added to the aggregated data profile for the Colorado Municipal Court Building.

[0264] At step 5, attribute combinations are identified and formed so as to provide support with respect to a desired activity, action, process or trait. This step may include the creation or loading of templates that specify the one or more attributes necessary with respect to a particular action, activity, process or trait. For example, for an e-commerce action, the template may request information pertaining to the Data Subject's age, sex, size and preferred color(s) as attributes. In another example involving a travel reservation function, the template may request information pertaining to the Data Subject's preferred means of air travel by coach, business class or first class as attributes. The privacy server may be loaded with or have access to a plurality of such templates in order to support a wide variety of differing actions, activities, processes and / or traits. In addition, the privacy server may be configured to facilitate the manual override of established templates if / as desired by the controlling entity and creation of new templates with respect to desired new actions, activities, processes and / or traits. Such manual override may occur for instance by means of a graphical user interface of a privacy client running on a Data Subject's mobile device. For instance, a Data Subject may use the graphical user interface to override the request for information pertaining to the Data Subject's preferred means of air travel by coach, business class or first class because in one example the Data Subject may be traveling by cruise ship and therefore the Data Subject may desire to specify whether he/she wants a suite, balcony stateroom, outside stateroom, or inside stateroom as attributes. In this example, the graphical user interface may permit the Data Subject to elect the minimal attributes for transmission from the Data Subject's aggregated data profile.

[0265] At step 6, requests are received by the privacy server from privacy clients that may reside on Data Subject devices, on service provider devices, accessible via and residing in a cloud network, or residing on the same computing device as the privacy server with regard to a specific action, activity, process or trait. The nature and substance of requests that may be received by the privacy server from privacy clients may vary in nature depending on a variety of factors comprising whether the system is implemented as DRMI, DRMD or otherwise, whether a request pertains to healthcare, education, mobile, financial, Web, Internet of Things or other applications, etc.

[0266] At step 7, a determination is made regarding the level of abstraction appropriate for the desired level of security, anonymity, privacy and relevancy with respect to a particular action, activity, process or trait. For example, the system may introduce an initial layer of abstraction by linking relevant data attributes, separating relevant data attributes into

one or more TDR as determined desirable with respect to a given action, activity, process or trait. Additional layers of abstraction may be introduced beyond separating data attributes into one or more TDR by means of abstracting individual attributes, attribute combinations, or both by replacing them with DDIDs that cannot be understood without access to replacement keys (RKs). The privacy, anonymity and security of attributes contained or referenced within a TDR may be further improved or enhanced by using known protection techniques such as encrypting, tokenizing, pseudonymizing and eliding and further layers of abstraction may be introduced by using additional DDIDs to refer to networks, internets, intranets, and third party computers that may be integrated, or communicate, with one or more embodiments of the present invention.

[0267] At step 8, desired attribute combinations are selected by a controlling entity from the privacy server based on the attributes associated with the applicable template as may be necessary with respect to a desired action, activity, process or trait. The abstraction module may determine desired attributes that may be controlled by the controlling entity or delegated to another entity as an authorized party, where the authorized party may choose to use the abstraction module to select attributes based on established templates, select attributes on the fly, or intelligently detect appropriate input, among other methods.

[0268] In one example of step 8, with an e-commerce site selling sports equipment, an internet browser provider that is acting as the controlling entity may use the abstraction module of the privacy server to determine that information regarding a Data Subject's height, weight and budget are needed for a receiving web site to give options for appropriate sports equipment such as kayaks and paddles.

[0269] At step 9, the abstraction module of the privacy server generates unique DDIDs or accepts or modifies temporally unique, dynamically changing values to serve as DDIDs and assigns a DDID to each attribute combination of operation 8, to form TDRs. These DDIDs may serve various functions including, but not limited to, replacement or simple association. For example, if the internet browser provider acting as the controlling entity instructs the abstraction module to create a TDR with a single layer of abstraction it may assign a DDID that is not visibly associated with other TDRs for the same Data Subject without access to association keys (AKs). As another example, if the internet browser provider acting as the controlling entity instructs the abstraction module to create a TDR with two layers of abstraction it may (i) assign DDIDs to be associated with the data attributes for the duration of the TDR and (ii) further abstract the data attributes by assigning a DDID of Ab5 to the Data Subject's weight, a DDID of 67h to the Data Subject's height and a DDID of Gw2 to the Data Subject's budget that cannot be understood without access to replacement keys (RKs). Step 9 may also include obtaining one or more attributes from one or more databases, the attributes relating to the Data Subject. The DDIDs utilized in step 9 may be confirmed as not being currently in use, and may be selected from expired, previously used DDIDs.

[0270] At step 10, TDRs comprised of attribute combinations and DDIDs are transmitted, by the privacy server via privacy clients to recipient entities for use by recipient entities in connection with desired actions, activities, processes or traits pertaining to recipient entities. In the above example for instance, the internet browser provider acting as the controlling entity may deliver to the ecommerce site as the recipient entity a TDR comprised of a DDID together with second level abstracted data attributes comprised of Ab5, 67h and Gw2.

[0271] At step 11, TDRs (which may be comprised of attribute combinations and DDIDs with respect to desired actions, activities, processes or traits) are received by recipient entities by means of privacy clients. To the extent that the intended use of the system is to enable creation of output for big data analytics, the receipt of the TDRs may be the last step (e.g., see the example of a potential embodiment of the invention discussed in the context of Figure Z to provide privatized/anonymized data for big data analytics so applicable Data Subject(s) have the "right to be forgotten"), however, more interactive use of TDRs may involve optional steps 12 through 17.

[0272] At optional step 12, TDRs (which may be comprised of attribute combinations and DDIDs for a desired online action, activity, process or trait) are interpreted by recipient entities by means of privacy clients and provide access to use of AKs and / or RKs as necessary to understand the contents of the TDRs. In the above example for instance, the ecommerce site as the recipient entity would access the RK information to understand the value attributed to Ab5 for the Data Subject's weight, the value attributed to 67h for the Data Subject's height and the value attributed to Gw2 to the Data Subject's budget.

[0273] At optional step 13, the privacy client may capture new data attributes associated with the desired online action, activity, process or trait that augment the original TDR data attributes as new information in TDR format.

[0274] At optional step 14, the privacy client may capture new data attributes associated with offline activity, if any, associated with the desired online action, activity, process or trait that augment the original TDR data attributes as new information in TDR format.

[0275] At optional step 15, privacy clients transmit TDRs comprised of DDIDs and attribute combinations pertaining to online/offline sessions back to the privacy server.

[0276] In the context of steps 14 and 15, since TDRs are transmitted via privacy clients to the privacy server without AKs or RKs they are transmitted in a disaggregated and anonymized format, so that, if someone intercepts the TDRs, they will not receive all data applicable to the Data Subject, desired action, activity, process or trait.

[0277] At optional step 16, in one example, re-aggregation of attribute combinations is performed through application by the maintenance module of relationship information between and among DDIDs and attribute combinations by means of association keys (AKs) and (DKs) residing at the privacy server. In the example, this would mean that the original or modified TDRs return to the privacy server, which may then modify or add the new information about recommended kayaks and paddles to the aggregated data profile for the Data Subject.

[0278] Upon completion of aforementioned re-aggregation of new data regarding the desired action, activity, process or trait from the attribute combinations, in one example the DDID may then be considered expired and reintroduced to the system at optional step 17 for reassignment and use with other attributes, attribute combinations, Data Subjects, actions, activities, processes, traits or data, forming new TDRs in the same fashion as described above.

[0279] For instance, the DDIDs Ab5, 67h and Gw2 assigned to the attributes in step 9 above may then be assigned to data attributes pertaining to other Data Subjects for instance in a like case hop or distant case leap manner. For example, a like case hop may include re-association of Ab5 to a second Data Subject of the same or similar weight as the initial Data Subject or re-association of a piece of data on weight or something involving the same number but not associated with the same Data Subject whereas a distant case leap may involve reassigning Ab5 to an unrelated data attribute awaiting an DDID.

[0280] In a second example of Figure 6, a physician may request blood pressure information pertaining to a specified Data Subject who is a patient as collected offline by a nurse and entered online into the Data Subject's aggregated data profile. This request may cause the abstraction module of the privacy server, as part of step 8 above, to extract the attribute combination composed of the most recently recorded systolic and diastolic blood pressure values for the Data Subject. As part of step 9, in lieu of specifying the Data Subject's identity, the privacy server may combine those attribute combinations with an DDID assigned by the privacy server to form a TDR. As part of step 10, the blood pressure attributes may be communicated to the physician together with the assigned DDID via the privacy client that may reside on a Data Subject device, on a service provider device, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server. At this point, the combination of the DDID and attribute combination pertaining to blood pressure would comprise the TDR. As part of step 12, the physician, as the recipient entity, may read the blood pressure values via means of the RKs and as part of steps 13 and 14 may record online and offline observations, recommendations or comments pertaining to the blood pressure reading as new data attributes. As part of step 15, the TDR augmented with online/offline information may be returned to the privacy server via the privacy client. As part of step 16, the privacy server may use the information to update the Data Subject's aggregated data profile. In this manner, an unintended recipient of the TDR would be unable to correlate the identity of the Data Subject and would only see the DDID which may be reassigned to another Data Subject in a like case hop or distant case leap manner after use by the physician.

[0281] Figure 6A shows an example of a process for providing data security, data privacy and anonymity, in accordance with one embodiment of the present invention involving interaction with external databases. Figure 6A shows process steps that may be implemented by a controlling party or a system, in one example.

[0282] At step 1 in Figure 6A, a third-party data source submits data that includes one or more data attributes pertaining to one or more Data Subjects as input to the system. It should be noted that, in the embodiment of the invention represented by Figure 6A, prior to submitting data that includes one or more data attributes pertaining to one or more Data Subjects input to the system, the third-party data source would have already created an aggregated data profile for each Data Subject (see, e.g., Figure 1A) which the third-party data source would maintain, directly or indirectly, in one or more databases.

[0283] At step 2, requests are received by the privacy server from privacy clients that may reside on Data Subject devices, on service provider devices, accessible via and residing in a cloud network, or residing on the same computing device as the privacy server with regard to a specific action, activity, process or trait. The nature and substance of requests that may be received by the privacy server from privacy clients may vary in nature depending on a variety of factors comprising whether the system is implemented as DRMI, DRMD or otherwise, whether a request pertains to healthcare, education, mobile, financial, Web, Internet of Things or other applications, etc.

[0284] The privacy, anonymity and security of attributes contained or referenced within a TDR may be further improved or enhanced by using known protection techniques such as encrypting, tokenizing, pseudonymizing and eliding and further layers of abstraction may be introduced by using additional DDIDs to refer to networks, internets, intranets, and third party computers that may be integrated, or communicate, with one or more embodiments of the present invention.

[0285] At step 3, a determination is made regarding the level of abstraction appropriate for the desired level of security, anonymity, privacy and relevancy for a particular action, activity, process or trait. For example, the system may introduce abstraction by means of abstracting individual attributes, attribute combinations, or both by representing them with DDIDs that cannot be understood without access to replacement keys (RKs). The privacy / anonymity and security of attributes contained or referenced within a TDR may be further improved or enhanced by using known protection techniques such as encrypting, tokenizing, pseudonymizing and eliding and further layers of abstraction may be introduced by using additional DDIDs to refer to networks, internets, intranets, and third party computers that may be integrated, or commu-

nicate, with one or more embodiments of the present invention.

[0286] At step 4, desired attribute combinations are selected by a controlling entity from the privacy server based on the attributes associated with the applicable template as may be necessary with respect to a desired action, activity, process or trait. The abstraction module may determine desired attributes that may be controlled by the controlling entity or delegated to another entity as an authorized party, where the authorized party may choose to use the abstraction module to select attributes based on established templates, select attributes on the fly, or intelligently detect appropriate input, among other methods.

[0287] In one example of step 4, in the context of healthcare research, a hospital that is acting as the controlling entity may use the abstraction module of the privacy server to obfuscate information regarding a Data Subject's height, weight and name before sending the information to a research facility.

[0288] At step 5, the abstraction module of the privacy server assigns a DDID to each attribute combination of operation 4, to form TDRs. These DDIDs may serve various functions including, but not limited to, replacement or simple association. For example, if hospital acting as the controlling entity instructs the abstraction module to create a TDR with two layers of abstraction it may abstract the data attributes by assigning a DDID of Ab5 to the Data Subject's weight, a DDID of 67h to the Data Subject's height and a DDID of Gw2 to the Data Subject's name that cannot be understood without access to replacement keys (RKs). Step 5 may also include obtaining one or more attributes from one or more databases, the attributes relating to the Data Subject. The DDIDs utilized in step 5 may be confirmed as not being currently in use, and may be selected from expired, previously used DDIDs.

[0289] At step 6, TDRs comprised of attribute combinations and DDIDs are transmitted, by the privacy server via privacy clients to recipient entities for use by recipient entities in connection with desired actions, activities, processes or traits pertaining to recipient entities. In the above example for instance, the hospital acting as the controlling entity may deliver to the research facility as the recipient entity a TDR comprised of abstracted data attributes comprised of Ab5, 67h and Gw2.

[0290] At step 7, TDRs (which may be comprised of attribute combinations and DDIDs with respect to a desired action, activity, process or trait) are received by recipient entities by means of privacy clients. In the above example for instance, the research facility as the recipient entity would receive the information for analysis but without divulging personally identifying information pertaining to weight, height. Rather, the research facility would receive Ab5, 67h and Gw2 that it could not decipher unless granted access to relevant RK information. To the extent that the intended purpose is big data analysis, the receipt of the TDRs may be the last step, however, more interactive use of TDRs may involve optional steps 8 through 13.

[0291] At optional step 8, TDRs (which may be comprised of attribute combinations and DDIDs with respect to a desired action, activity, process or trait) are interpreted by recipient entities by means of privacy clients and provide access to use of AKs and / or RKs as necessary to understand the contents of the TDRs.

[0292] At optional step 9, the privacy client may capture new data attributes associated with respect to the desired online action, activity, process or trait that augment the original TDR data attributes as new information in TDR format.

[0293] At optional step 10, the privacy client may capture new data attributes associated with offline activity, if any, associated with the desired online action, activity, process or trait that augment the original TDR data attributes as new information in TDR format.

[0294] At optional step 11, privacy clients transmit TDRs comprised of attribute combinations and DDIDs pertaining to online / offline sessions back to the privacy server. Since TDRs are transmitted via privacy clients to the privacy server without AKs and / or RKS they are transmitted in a disaggregated and anonymized format so if someone intercepts the TDRs they will not receive all data applicable to the Data Subject, or desired action, activity, process or trait.

[0295] At optional step 12, in one example, re-aggregation of attribute combinations is performed through application by the maintenance module of relationship information between and among DDID and attribute combinations by means of association keys (AKs) and / or replacement keys (RKs) residing at the privacy server. In the example, this would mean that the original or modified TDRs return to the privacy server, which may then modify or add the new information about recommended kayaks and paddles to the aggregated data profile for the Data Subject.

[0296] Upon completion of aforementioned re-aggregation of new data regarding the desired action, activity, process or trait from the attribute combinations, in one example the DDID may then be considered expired and reintroduced to the system at optional step 13 for reassignment and use with other attributes, attribute combinations, Data Subjects, actions, activities, processes, traits, or data, forming new TDRs in the same fashion as described above.

[0297] Figure 6B shows how potential embodiments of the present invention may provide dynamic anonymity for data elements contained in one or more databases (whether the one or more databases are internal to the system as illustrated in Figure 1A and / or external to the system as illustrated in Figure 1B) that are considered too sensitive to be revealed in an identifiable manner external to an organization - e.g., data which directly identifies a Data Subject or sensitive action, activity, process and / or trait (a direct identifier) or indirectly identifies a Data Subject or sensitive action, activity, process and / or trait when combined with other data (a quasi-identifier). The system may dynamically obscure said sensitive data when exposed externally to the organization by replacing said data with one or more DDIDs. Keys necessary

to understand the association between the one or more DDIDs and the obscured sensitive data may then be kept securely in a Circle of Trust (CoT) and only made available to authorized parties. DDIDs may be "designed" (i.e., the data obscuring strategy may be tailored in such a way) to allow varying levels of data use / analysis of DDIDs consistent with PERMS established by a Data Subject or Trusted Party without revealing underlying sensitive data. The sensitive data represented by the one or more DDIDs may not be disclosed until keys are requested by one or more parties that have been authorized by the Data Subject or Trusted Party to receive and / or make use of the underlying sensitive data.

[0298] In one potential embodiment of the present invention, the obscuring of sensitive data as described above may occur only with respect to a certain computer application that requests data from the subject one or more databases by intercepting requests for sensitive data from the one or more database(s) at the presentation layer of said computer application and replacing the sensitive data with one or more DDIDs as described above. In another potential embodiment of the present invention, obscuring of sensitive data may occur with respect to one or more computer applications that request data from the subject one or more databases by intercepting requests for sensitive data at the one or more database(s) connection level(s) and replacing the sensitive data with one or more DDIDs as described above.

[0299] Figure 6B shows process steps that may be implemented by a controlling party or a system to obscure sensitive data, in one example.

[0300] At step 1 in Figure 6B, requests are received by the privacy server from privacy clients that may reside on Data Subject devices, on service provider devices, accessible via and residing in a cloud network, or residing on the same computing device as the privacy server with regard to data elements contained in one or more databases (whether the one or more databases are internal to the system as illustrated in Figure 1A and / or external to the system as illustrated in Figure 1B) considered too sensitive to be revealed in an identifiable manner external to an organization - e.g., data which directly identifies a Data Subject or sensitive action, activity, process and / or trait (a direct identifier) or indirectly identifies a Data Subject or sensitive action, activity, process and / or trait when combined with other data (a quasi-identifier). The nature and substance of requests that may be received by the privacy server from privacy clients may vary in nature depending on a variety of factors comprising whether the system is implemented as DRMI, DRMD or otherwise, whether a request pertains to healthcare, education, mobile, financial, Web, Internet of Things or other applications, etc.

[0301] At step 2, the abstraction module determines the level of abstraction appropriate for the desired level of security, privacy, anonymity and relevancy for the sensitive data elements consistent with PERMS established by a Data Subject or Trusted Party and DDID association strategies are developed for the sensitive data elements consistent with the scope of data use / analysis permitted by said PERMS.

[0302] At step 3, the one or more DDIDs determined by the abstraction module to dynamically obscure the sensitive data elements are sent to the privacy client.

[0303] At step 4, the one or more sensitive data elements are dynamically obscured by replacing said data elements with one or more DDIDs determined by the abstraction module and resulting DDIDs are used to replace the sensitive data elements in data communicated externally to the organization. In one example of step 3, the obscuring of sensitive data elements occurs only with respect to a certain computer application that requests data from the subject one or more databases by intercepting requests for sensitive data from the one or more database(s) at the presentation layer of said computer application and replacing the sensitive data with one or more DDIDs as determined by the abstraction module. In another example of step 3, the obscuring of sensitive data elements occurs with respect to one or more computer applications that request data from the subject one or more databases by intercepting requests for sensitive data from the one or more database(s) at the one or more database(s) connection level(s) and replacing the sensitive data with one or more DDIDs as determined by the abstraction module.

[0304] At step 5, keys necessary to understand the association(s) between the one or more DDIDs and the obscured sensitive data elements are securely stored in a Circle of Trust (CoT).

[0305] At step 6, keys necessary to understand the association(s) between the one or more DDIDs and the obscured sensitive data elements that are securely stored in a Circle of Trust (CoT) are made available only to authorized parties. Sensitive data represented by the one or more DDIDs is not be disclosed until keys are requested by one or more parties that have been authorized by the Data Subject or Trusted Party to receive and / or make use of the underlying sensitive data.

[0306] Figure 7 shows an example of process steps that may be implemented by a recipient entity, in one example of the present disclosure.

[0307] At step 1, a TDR comprised of attribute combinations selected by the controlling entity combined with a DDID to be associated with the data attributes for the duration of the TDR are received by a recipient client by means of a privacy client residing on a Data Subject device, on a service provider device, accessible via and residing in a cloud network, or residing on the same computing device as the privacy server indicating a request with respect to a desired action, activity, process or trait. For instance, in the kayak example above, the e-commerce site receiving entity may receive the Data Subject's TDR request with respect to a desired action, activity, process or trait.

[0308] At step 2, TDRs (which may be comprised of attribute combinations and DDIDs for the desired online action,

activity, process or trait) are interpreted by the recipient entity by means of a privacy client that provides access to use of AKs and / or RKs as necessary to understand the contents of the TDRs. In the above example for instance, the ecommerce site would access the RK information residing on Data Subject devices, on service provider devices, accessible via and residing in a cloud network, or residing on the same computing device as the privacy server to understand the value attributed to Ab5 for the Data Subject's weight, the value attributed to 67h for the Data Subject's height and the value attributed to Gw2 to the Data Subject's budget.

[0309] At step 3, in one example the receiving entity may use the TDR information it has received to customize a response to the Data Subject's transmitted attributes. In the kayak example, this would allow the ecommerce site to use the information to give the Data Subject suggestions on which kayak and paddle to purchase.

[0310] At step 4, in one example the privacy client captures data for online activity performed at the recipient entity that is associated with attribute combinations by means of access to a privacy client that may be residing on a Data Subject device, on a service provider device, accessible via and residing in a cloud network, or residing on the same computing device as the privacy server.

[0311] At step 5, in one example, the recipient entity captures data for offline activity, if any, associated with attribute combinations and converts this into online data. In an instance such as the kayak example, if the Data Subject is also a loyalty rewards member at physical store locations also operated by the ecommerce site and has opted to let other preferences be known, the receiving entity may further augment the received data with this online component.

[0312] At step 5, in one example, the privacy client then transmits data pertaining to online sessions and offline activity associated with attribute combinations and DDIDs in disaggregated and anonymized format to the privacy server.

[0313] At step 6, since the DDID components of TDRs are reintroduced to the system for reassignment and use with other attributes, attribute combinations, Data Subjects, actions, activities, processes, traits, or data, forming new TDRs in the same fashion as described above, the recipient entity may see the same DDID at a later time but the DDID may have no connection to any other TDR associated with the Data Subject or otherwise with regard to which it was previously associated. For example, later that day or week the ecommerce site may see the same DDID again but attached to different information pertaining to an entirely different Data Subject.

[0314] In a second example of Figure 7, the physician requesting the blood pressure information may receive, as part of step 1 via the privacy client, a TDR comprised of the most recently recorded systolic and diastolic blood pressure values and the DDID assigned by the privacy server to the Data Subject. As part of steps 2 and 3, the physician is able to read the blood pressure information. As part of steps 4 and 5, the physician may add observations, recommendations or comments pertaining to the blood pressure that as part of step 6 would then be sent to the privacy server via the privacy client that may be residing on a Data Subject device, on a service provider device, accessible via and residing in a cloud network, or residing on the same computing device as the privacy server.

[0315] Figure 8 illustrates an example of a process to verify authority to proceed with respect to an action, activity, process or trait at a particular time and / or place, in accordance with one embodiment of the present invention.

[0316] At step 1, in one example a recipient entity transmits a request to the privacy server via a privacy client that may be residing on a Data Subject device, on a service provider device, accessible via and residing in a cloud network, or residing on the same computing device as the privacy server requesting the privacy server to confirm whether an undisclosed Data Subject or related party associated with a TDR is authorized to participate with respect to an action, activity, process or trait at a particular time and / or place. For instance, when after looking through the recommended kayaks and paddles on the e-commerce site, the related party is ready to make a purchase, the e-commerce site may query the authentication module of the privacy server to determine whether the related party is authorized to consummate the requested transaction.

[0317] At step 2, in one example the authentication module of the privacy server compares the DDID included in the TDR to a list of authorized DDIDs contained in a database to determine authorization of the Data Subject or related party to participate with respect to a desired action, activity, process or trait at the specified time and / or place. In terms of the kayak example, the authentication module of the privacy server may ensure that the DDIDs being used are still active and authorized, thereby indicating that the Data Subject or related party is authorized to consummate the desired transaction.

[0318] Optionally, at step 3, in one example the privacy server may request the party in control of a privacy client that may reside on a Data Subject device, on a service provider device, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server, in this case the e-commerce site, to confirm they are authorized to participate in the desired transaction.

[0319] If optional step 3 is invoked, in one example step 4 checks to determine if the party in control of the privacy client is verified as being authorized. For example, in order to avoid deceptive attempts to acquire information such as usernames, passwords, or credit card details by masquerading as a trustworthy entity (also known as "phishing"), step 4 may require verification by the e-commerce site that it is an authorized reseller of the kayak equipment by means of known confirmation techniques.

[0320] At step 5, in one example, if verification is obtained, the authentication module of the privacy server transmits

the authorization status information to the party in control of the privacy client.

[0321] At step 6, in one example the authorization status information is used to allow or deny proceeding with respect to a desired action, activity, process or trait.

[0322] At step 7, once the authentication function has been carried out and the optional additional verification steps are completed, the privacy server sends via a privacy client the AK and / or RK information necessary to interpret TDR content so that the related party may purchase the desired products and the transaction may be processed by the receiving entity, which in above example may be the ecommerce site.

[0323] In a second example of Figure 8, a physician may send a TDR to the privacy server via a privacy client to verify whether a Data Subject that is a patient is authorized to participate in an explorative study. This would cause the authentication module of the privacy server, as part of step 2, to compare the Data Subject's DDID in the TDR to a list of authorized DDIDs contained in a database to determine if the Data Subject is authorized to participate in the study. Optionally, at step 3 the authentication module of the privacy server may request the physician submitting the request to confirm they are authorized to request that the Data Subject be a participant in the explorative study. If optional step 3 is invoked, step 4 checks to determine if the physician is authorized by means of known confirmation techniques such as password confirmation or multi-factor authentication. In step 5, if verification is obtained, the authentication module of the privacy server may transmit the authorization status information via the privacy client and in step 6 the authorization status may be used to allow or deny the request for the Data Subject to participate in the explorative study and step 7 would provide access to AK and / or RK key information necessary to interpret TDR content and proceed.

[0324] Figure 9 illustrates an example of a process of withholding replacement key (RK) or association key (AK) information or other protective information unless verified, in accordance with one embodiment of the present invention. As shown at step 1, in one example the party in control of a privacy client including a TDR transmits to the authentication module of the privacy server via a privacy client that may be residing on a Data Subject device, on a service provider device, accessible via and residing in a cloud network, or residing on the same computing device as the privacy server a request for AKs and / or RKs, and / or keys necessary to unlock TDR data attributes protected using other techniques such as encrypting, tokenizing, pseudonymizing or eliding.

[0325] In the kayak example, data may be sent using various additional steps to protect it in transit, however, the receiving entity e-commerce site may need the key(s) to unlock and / or associate the three pieces of information regarding height, weight and budget initially sent to it by the privacy client. At step 2, in one example, the authentication module of the privacy server compares TDR recipient attribute combinations to authorized recipient attribute combinations to determine whether the TDR recipient is an authorized recipient. If the authentication module of the privacy server verifies that TDR recipient attribute combinations matches authorized recipient attribute combinations, then the authentication module of the privacy server transmits to the TDR recipient as part of step 3, via a privacy client, in one example, the keys necessary to unlock the TDR.

[0326] In a second example of Figure 8, in step 1 a physician receiving an encrypted, tokenized or elided TDR containing requested blood pressure information may be required to send a TDR to the authentication module of the privacy server via a privacy client to verify that the physician is authorized to view the requested information. At step 2 the authentication module of the privacy server may compare the physician's TDR information to authorized recipient attribute combinations to determine whether the physician is an authorized recipient. If the authentication module of the privacy server verifies that the physician's TDR information matches authorized recipient attribute combinations, then the authentication module of the privacy server may transmit to the physician via a privacy client the keys necessary to unlock applicable protection techniques for the encrypted, tokenized or elided TDR containing requested blood pressure information.

[0327] Figure 10 illustrates an example of analyzing interests of related parties in an anonymous fashion in accordance with one embodiment of the present invention. At step 1, in one example, related parties (RPs) select attribute combinations (ACs) to be shared with merchants/service providers via privacy clients on mobile and / or wearable devices. For example, rather than utilizing an ecommerce site, a related party may go to a physical location of an outdoor sporting store and share the same information about height, weight and budget via a mobile or wearable device.

[0328] At step 2, in one example, the privacy server may assign DDID(s) to the attribute combinations to form TDR(s) on privacy clients resident on mobile / wearable / portable devices.

[0329] At step 3, in one example, the TDR(s) are transmitted to the merchant/service provider recipient entity(s) via privacy clients resident on mobile / wearable / portable devices. As an example with the kayaks, the store may receive the three separate TDR enabled data attributes via in-store devices, beacons or the like from a mobile / wearable / portable device of a Data Subject.

[0330] At step 4, in one example merchant/service provider recipient entity(s) may view attribute combinations authorized by related parties and transmitted to the merchant/service provider recipient entity(s) by privacy clients resident on mobile / wearable / portable devices. For instance, the store may view the height, weight and budget of the related party.

[0331] At step 5, in one example, the merchant/service provider recipient entity(s) may make offers to Data Subjects and / or related parties on an anonymous basis without yet knowing the identity of the Data Subjects and / or related parties.

[0332] At step 6, in one example, Data Subjects and / or related parties may elect to respond to merchant/service

provider recipient entity(s) offers that they find desirable and consummate transactions.

[0333] The system and methods described herein may provide related parties with a way to achieve greater anonymity and increased privacy / anonymity and security of data while utilizing one or more communication networks. Without these systems and methods, third parties may be able to obtain the true identity of Data Subjects or related parties based on their activity on the communication networks via network services and / or technology providers that have associated identifying information with the activity of the Data Subjects or related parties on and / or between the networks.

[0334] Disclosed herein are other various methods for providing data security and data privacy / anonymity. In one example, a method may include the steps or operations of receiving, at a computing device, an electronic data element; identifying one or more data attributes with the electronic data element; selecting, through the computing device, a DDID; associating the selected DDID with one or more of the data attributes; and creating a TDR from at least the selected unique DDID and the one or more data attributes.

[0335] In one example, the step of selecting a data element includes generating the unique DDID or in another example accepting or modifying a temporally unique, dynamically changing value to serve as the DDID. In one example, the method may also include causing the association between the selected DDID and the one or more data attributes to expire. In another example, the method may include storing, in a database accessible to the computing device, information regarding the time periods during which the selected unique DDID was associated with different data attributes or combinations of attributes. In another embodiment, the method may also include re-associating the selected unique DDID with the one or more data attributes following expiration of the association between the DDID and the one or more data attributes. In one example, the expiration of the DDID occurs at a predetermined time, or the expiration may occur following completion of a predetermined event or activity. In another example, the TDR may be authorized for use only during a given time period or at a predetermined location. In another example, the method may include changing the unique DDID assigned to the one or more data attributes, wherein the changing of the unique DDID may occur on a random or a scheduled basis, or may occur following the completion of a predetermined activity or event.

[0336] Another method is disclosed herein for facilitating transactions over a network. In one example, the method may include operations of receiving a request, at a privacy server, from a client device to conduct activity over a network; determining which of a plurality of data attributes in a database are necessary to complete the requested activity; creating a DDID; associating the DDID with the determined data attributes to create a combined TDR; making the combined TDR accessible to at least one network device for conducting or initiating the requesting activity; receiving a modified TDR that includes additional information related to the activity performed; and storing the modified TDR in the memory database. In another method implementation, disclosed herein is a method of providing controlled distribution of electronic information. In one example, the method may include receiving a request at a privacy control module to conduct an activity over a network; selecting attributes of Data Subjects located in a database accessible to the privacy control module determined to be necessary to fulfill the request, wherein other attributes of the Data Subject which are not determined to be necessary are not selected; assigning a DDID to the selected attributes and the Data Subject or Data Subjects to which they apply with an abstraction module of the privacy control module, wherein the DDID does not reveal the unselected attributes; recording the time at which the unique DDID is assigned; receiving an indication that the requested activity is complete; receiving the unique DDID and the determined attributes and the Data Subject or Data Subjects to which they apply at the privacy control module, wherein the attributes are modified to include information regarding the conducted activity; and recording the time at which the conducted activity is complete and the unique DDID and the determined attributes and the Data Subject or Data Subjects to which they apply are received at the privacy control module.

[0337] In one example, the method may also include assigning an additional DDID to one or more of the selected attributes or Data Subjects. In another example, the method may include re-associating, using the recorded times, the unique DDID and data attributes with the true identity of the Data Subjects. The method may also include reassigning the unique DDID to other data attributes, and recording the time at which the unique DDID is reassigned.

[0338] Another method is disclosed herein for improving data security. In one example, the method may include associating the Data Subject with at least one attribute; and associating a DDID with the at least one attribute to create a TDR; wherein the TDR limits access to attributes of the Data Subject to only those necessary to perform a given action. In one example, the method may include assigning an association key (AK) and / or replacement key (RK) to the TDR, wherein access to the AK and / or RK is required for authorized access to TDR. In another example, the method may also include causing the association between the DDID and the at least one attribute to expire, wherein the expiration occurs at a predetermined time and / or the expiration may occur following completion of a predetermined event or activity. In another embodiment, the method may include re-associating the DDID with the at least one different attribute following an expiration of the association between the DDID and the at least one attribute. The method may also include storing, in a database, information regarding one or more time periods during which the DDID was associated with different data attributes or combinations of attributes.

[0339] Various approaches may be used to associate DDIDs with different attribute combinations to form TDRs. The DDIDs may have a certain or variable length, and may be made up of various code composition elements such as

numbers, characters, cases, and / or special characters. In addition, the DDIDs may be generated in random or consistent intervals. In one example, only authorized parties with access to association keys (AKs) and / or replacement keys (RKs) maintained by the maintenance module necessary to re-aggregate the otherwise disaggregated attribute combinations will have the capability to determine which attribute combinations are properly associated with other attribute combinations, Data Subjects, related parties, or aggregated data profiles. However, sites may still track and utilize the attribute combinations contained within TDRs in real time, with the understanding that they have a temporally limited existence and that associated DDIDs may be reused later for different actions, activities, processes, traits, attribute combinations, Data Subjects and / or related parties.

[0340] The attribute combinations transmitted may include single or various combinations of explicit data, personally identifying information (PII), behavioral data, derived data, rich data or other data.

Example A.

[0341] In a first example, a system may be configured so that a related party is the controlling entity authorized to designate to which other parties attribute combinations will be released. Example A illustrates how the system processes information generated by a related party (related party X or "RP X") that engages in four different online sessions with two different service providers ("SP"s) from various industries over three different Communication Networks ("CN"s). Figures 11-20 illustrate this example, and show how information may be managed at various stages and under various circumstances, in one example of an embodiment of the invention. It is understood that Figures 11-20 are provided by way of example only, and that embodiments of the present invention may be implemented in ways different than shown in the examples of Figures 11-20.

[0342] Figure 11 shows an example wherein related party X transmits attribute combination A (Explicit Data) to a website Service Provider such as Pandora Radio ("SP1") via online internet access ("Communication Network 1" or "CN1"). Attribute combination A is assigned an identifier code of DDID 1 (for a limited temporal period) by the abstraction module of the privacy server ("PS"). The identifier code together with attribute combination A is communicated to SP1 via CN1 via a security client. In Figure 11, the combination of DDID 1 and attribute combination A represent a TDR for related party X for the limited temporal period.

[0343] Figure 12 shows an example wherein when interacting with SP1, related party X generated activity information (Behavioral Data) tracked by SP1 that was transmitted as attribute combination A1 by a privacy client that may reside on a Data Subject device, on a service provider device, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server back to the privacy server. The maintenance module of the privacy server may maintain information regarding attribute combinations and various DDID codes assigned to each attribute combination over time and at different points in time, as well as the CN and SP associated with each attribute combination. In Figure 12, the combination of DDID 1, attribute combination A, and attribute combination A1 represent a TDR for related party X for the limited temporal period of the association between DDID 1, attribute combination A, and attribute combination A1. Upon completion of the association of the new data regarding the desired action, activity, or process from the attribution combinations, DDID 1 may be reassigned for use in a new TDR. The combination of DDIDs and attribute combinations shown in Figures 13 through 20 also represents TDRs for the temporal period of the association between the DDIDs and attribute combinations.

[0344] Figure 13 shows an example where related party X transmits another attribute combination E (Explicit Data) to Pandora Radio ("SP1") via Online Internet Access ("CN1"). Attribute combination E is assigned an identifier code of DDID 4, for a limited temporal period, by the privacy server ("PS") and the identifier code together with attribute combination E is communicated to SP1 via CN1 via a security client.

[0345] Figure 14 shows an example wherein when interacting with SP1 in this example, related party X generated activity information (Behavioral Data) tracked by SP1 that was transmitted as attribute combination E1 back to the abstraction module of the privacy server via a privacy client that may reside on a Data Subject device, on a service provider device, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server.

[0346] Figure 15 shows an example wherein related party X transmitted attribute combination Q (Explicit Data) to another version of the SP1 Pandora Radio in mobile application form, accessible via mobile device access communications ("Communication Network 2" or "CN2"). Attribute combination Q is assigned an identifier code of DDID 9, for a limited temporal period, by the privacy server and the identifier code together with attribute combination Q is communicated as a TDR to SP 1 via CN2 via a security client.

[0347] Figure 16 shows an example wherein when interacting with SP1, related party X generated activity information (Behavior Data) tracked by SP1 that was transmitted as attribute combination Q1 back to the abstraction module of the privacy server via a privacy client that may reside on a Data Subject device, on a service provider device, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server.

[0348] Figure 17 shows an example wherein party X transmits attribute combination P (Behavioral Data) via a privacy

client that may reside on a Data Subject device, on a service provider device, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server to a Service Provider ("SP2") that provides monitoring services related to exercise activity such as FitBit via wearable device access communications ("Communication Network 3" or "CN3"). Attribute combination P is assigned an identifier code of DDID 7, for a limited temporal period, by the PS and the identifier code together with attribute combination P is communicated as a TDR to SP2 via CN3 via a security client.

[0349] Figure 18 shows an example wherein when interacting with SP2 in this situation, SP2 calculated the percentage of desired daily calorie burn (Derived Data) accomplished by related party X, and that this information was transmitted via a privacy client that may reside on a Data Subject device, on a service provider device, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server as attribute combination PI back to the privacy server.

[0350] Figure 19 shows an example wherein the attribute combinations accessible to each SP as well as the attribute combinations are re-transmitted by privacy clients that may reside on a Data Subject device, on a service provider device, accessible via and reside in a cloud network, or reside on the same computing device as the privacy server back to the privacy server. Figure 19 highlights that sessions of use within or between SPs may be subset between or within sessions so that without access to the security association keys that may be maintained by the maintenance module, SPs do not have in one example the information necessary to determine associations between the attribute combinations. However, they do have access to the attribute combinations created during each limited temporal period as determined by changing DDIDs, in one example. For example, SP1 does not know that DDID 1 and DDID 9 both pertain to related party X who accessed the two different versions of the website maintained by SP1 - one accessed via online internet access and the other accessed via mobile device access.

[0351] Figure 20 shows an example wherein the data accessible to related party X that includes all information sent to and retransmitted from the SPs. Figure 19 highlights that with access to the security association keys that may be maintained by the maintenance module, related party X, as the controlling entity, may have in one example the information necessary to determine associations between the attribute combinations for aggregation and normalization purposes. In addition, related party X may have the information to use, or have a data facilitator use, the maintenance module to perform further analysis and processing of the data in a secure environment. The new attribute combination Z represents new data ("Rich Data") that was produced by the maintenance module at the request of related party X by comparing all data associated with DDID 1, DDID 9, DDID 4 and DDID 7 to predict what other music choices related party X may enjoy that will assist in helping to attain the desired daily calorie burn. The attribute combination Z may include a list of the other music choices produced from this prediction, as well as data associated with the various other DDIDs. Attribute combination Z will not be communicated to any party (SP1, SP2 or otherwise) until desired by related party X, which is acting as the controlling entity. When related party X desires to share attribute combination Z, in one example it would be assigned a DDID code prior to transmission to the recipient parties designated by related party X. This new attribute combination will be more holistic and current when and if it is distributed to recipient entities as determined by the related party X.

Example B

[0352] In a second example shown in Figures 21-22, a system is configured so that a service provider ("SP3") is the controlling entity authorized to designate parties to whom select attribute combinations related to SP3 clients are released. SP3 may use the system to provide improved protection for its client's identity and privacy / anonymity. This includes reducing the likelihood of consumer or government backlash as a result of potential loss of privacy or anonymity, as well as increasing market penetration, use and acceptance of SP3 offerings. It is understood that Figures 21-22 are provided by way of example only, and that embodiments of the present invention may be implemented in ways different than shown in the examples of Figures 21-22.

[0353] Figures 21 and 22 show an example wherein SP3 provides each of a input technology vendor such as a website company that helps to capture order information ("ITV"), a process technology vendor such an online electronic payment processor ("PTV") and an output technology vendor such as a party that delivers selected products electronically to customers ("OTV") with only those attribute combinations necessary to perform the services assigned to each vendor. None of the vendors have access to Personally Identifying Information ("PII") that would reveal the identity of SP3 clients.

[0354] Figure 23 illustrates an example of implementation of dynamically created, changeable, and re-assignable DDIDs in the area of Internet behavioral ad serving. Without the benefit of some embodiments of the present invention, Internet behavioral ad serving is based primarily on ad networks placing cookies in a user's web browser and building a profile of said user by tracking user-visited websites that carry ads from the same ad network. In this manner, networks build a profile of user-visited websites augmentable with data from other sources, leading to detailed profiles of users for whom they have cookie information.

[0355] Typically, when a user visits a website ("Website1") in Figure 23 for the first time, said website: (i) delivers

content from the website to the user's browser; (ii) sends a cookie to the user's browser; and (iii) directs the user's browser to a web address to retrieve ad content to be served on the website from the ad network ("Ad Network 1"). The cookie delivered in (ii) above is referred to as a "First Party Cookie" since it relates to a website selected by the user. First Party Cookies can be beneficial to a user to help keep "state" information such as log-in progress, items in a shopping basket and other relevancies that improve the user's experience. When the user's browser requests ad information from Ad Network 1 as part of (iii) above, Ad Network 1 sends an ad to the user's browser that is displayed as part of Website1. If this is the first time the user's browser requests ad content from Ad Network 1, Ad Network 1 will also send a cookie to the user's browser. This cookie is referred to as a Third Party Cookie because it is not from a web page intended to be visited by the user. If Ad Network 1 has not previously tracked the user, Ad Network 1 will serve an ad based on traditional ad delivery technology (e.g., the nature of content on Website1 might be delivered). As the user visits more and more websites with ads served by Ad Network 1, Ad Network 1 (via the Third Party Cookie sent by Ad Network 1 to the user's browser) builds a profile of the behavioral data on the user based on the pages visited, time spent on each page and other variables such as information from the user's social network, online or offline buying behavior, psychographics and demographics together with further user information collected either by Ad Network 1's actions or by integrating information available from third party data providers. Based on the profile of the user created and managed by Ad Network 1, Ad Network 1 is able to display an ad targeted to the user based on what Ad Network 1 determined was of highest interest to the user.

[0356] This conventional tracking of the user from site to site and page to page by third party Ad Networks has raised privacy / anonymity concerns. In response, the Do-Not-Track (DNT) effort was launched through the World Wide Web Consortium (W3C), an international body in which member organizations, a full-time staff, and the public work together to develop Web standards for adoption by a cross section of regulators, civil society and commercial entities. The major browsers (i.e., IE, Chrome, Firefox, Safari) now offer a DNT option; however, no agreement exists on how recipient websites should respond to a DNT preference.

[0357] Despite this, some providers have recognized that DNT applies to third party website tracking - not first party website tracking. Under the draft W3C standard, If a first party receives a DNT:1 signal, the first party may engage in its normal collection and use of data. This includes the ability to customize the content, services, and advertising in the context of the first party experience. Under this recommendation, the first party must not share data about this network interaction with third parties who could not collect the data themselves; however, data about the transaction may be shared with service providers acting on behalf of the first party.

[0358] In Do-Not-Track situations, when a user visits a website ("Website1") the user's browser sends a notification to Website1 that the user is not to be tracked; and Website1 sends to the user's browser a First Party Cookie and content, plus the address where the browser should request the ad to be served on Website1 from an ad network ("Ad Network 1"). Ad Network 1 receives the request to not be tracked and sends the ad content to the user's browser, but no Third Party Cookie is placed on the user's browser. The ad is provided to the user based on traditional methods of targeting which may include, without limitation, targeting an ad to the content of the page (i.e., contextual targeting). Depending on how Do-Not-Track is implemented, as stated above, with respect to first parties, the consensus places few limitations on first parties (except that the first party must not share data about a DNT user's network interaction with third parties who could not collect the data themselves).

[0359] In contrast, with embodiments of the present invention, Do-Not-Track may be implemented to protect a related party's user's privacy / anonymity while still delivering content and targeted ads to support the primary revenue model of the Internet. Figure 23 represents one of a number of potential implementations of the present invention for ad serving.

[0360] At Step 1 in Figure 23, in one example a Data Subject or related party visits Website 1 for the first time and the browser sends a Do-Not-Track header to Website 1. If desired by the Data Subject or related party, the browser can also send a TDR to Website 1, thus enabling it to include "state" information for improving the Data Subject or related party's experience there. Website 1 then sends the content to the Data Subject or related party's browser.

[0361] At Step 2, in one example the Data Subject or related party's browser requests an ad for Website 1 from Ad Network 1 (with or without a TDR). When the TDR is not sent, the Data Subject or related party will receive a traditionally targeted ad from Ad Network 1 based on the page's content. When the TDR is sent, Ad Network 1 becomes enable to serve a highly targeted ad to the Data Subject or related party's browser based on the Data Subject or related party's relevant attributes. In this respect, the ad served by Ad Network 1 based on a TDR is likely more relevant to the Data Subject or related party than an ad served traditionally or by aggregated (and therefore more generally inferential) behavioral profile information the Ad Network would otherwise have collected on the Data Subject or related party.

[0362] At Step 3, in one example, as the Data Subject or related party visits additional sites ("WebsiteN"), a process similar to that in Steps 1 and 2 will occur. When the TDR is included, the website content and the ad content will be highly targeted; however, at a minimum Ad Network 1 will have no ability to collect information on or track the Data Subject or related party. Further, via the privacy client resident on the browser or through other mechanisms, the TDR may be included in the information sent to the website or to Ad Network 1.

[0363] In summary, under existing ad targeting technology, users may be tracked everywhere they go online, yet they

are served ads based on aggregated data out of which the ad network makes inferences about the particular user's preferences. This results in no user privacy / anonymity and low-to-moderate ad relevance. By combining aspects of the present invention and Do-Not-Track, users are empowered decide what information gets sent to which websites and ad networks. This not only enhances privacy / anonymity, but also ad relevance (for users) and improves sell-through and return on investment for merchants.

[0364] Figures 24 and 25 illustrate potential benefits of some embodiments of the present disclosure in the area of healthcare. Figure 24 highlights how temporally unique and purpose limited data representations (TDRs) may be used in one potential implementation of the invention to protect the confidentiality and privacy / anonymity of user and patient personally identifiable information (PII) and / or personal health information (PHI) in a healthcare information system. With the benefit of one embodiment of the present invention, a healthcare system may generate real-time TDRs that do not reveal sensitive PII/PHI without losing the context of, or access to, such information. In step 1.0, information may be received as input to the system including PII/PHI relevant to the registration process. In order to protect the privacy / anonymity of sensitive PII/PHI information, output from the registration process may replace PII/PHI user information [A] with TDRs (comprised of dynamically changing and re-assignable DDIDs and the PII/PHI information) without revealing the PII/PHI information so sensitive PII/PHI data is not exposed. This user data (including TDRs in lieu of PII/PHI information) would then be used as input to create, augment or alter the user data file at D1 without revealing PII/PHI information

[0365] [B]. Similarly, PII/PHI information that is output from the step 2.0 reservation process may be replaced with TDRs (comprised of dynamically changing and re-assignable DDIDs and the PII/PHI information) without revealing the PII/PHI information so sensitive PII/PHI data is not exposed. This clinical data (including TDRs in lieu of PII/PHI information) would then be used as input to create, augment or alter the clinical data file at D2 without revealing PII/PHI information [C]. Clinical data from D2 (after undergoing the clinical information search process at step 3.0) may then be combined with User data from D1 as input to the step 4.0 user profile search process without revealing PII/PHI information by means of access to and use of the temporally unique and purpose limited TDRs only. PII/PHI user information components of output resulting from the step 4.0 user profile search process may be replaced with TDRs (comprised of dynamically changing and re-assignable DDIDs and the PII/PHI information) without revealing the PII/PHI information so sensitive PII/PHI data is not exposed. Lastly, user data at D1 (including TDRs in lieu of PII/PHI information) can be used as input to the step 5.0 reservation record browse process without revealing PII/PHI information by means of access to and use of the temporally unique and purpose limited TDRs only. When access to detailed information from the user data file and / or clinical data file is required for authorized healthcare or ancillary service purposes, association keys (AKs) and / or replacement keys (RKs) may be used to discern the relevant sensitive PII/PHI data associated with applicable TDRs and DDIDs.

[0366] Figure 25 illustrates an example wherein dynamically created, changeable and re-assignable TDRs (comprised of dynamically changing and re-assignable DDIDs and the PII/PHI information) could be used to protect the confidentiality and privacy / anonymity of PII/PHI contained in patient medical records. Figure 25 shows how implementing the present invention with multiple levels of abstraction establishes "rings of privacy" such that only the level of identifying information necessary to perform a desired service or permitted function is provided. In this example, each of the Provider, State, Multi-State and National levels would receive attribute combinations appropriate for their respective permitted purposes. Temporally unique and purpose limited data representations (TDRs) may be used to protect the confidentiality and privacy / anonymity of user and patient personally identifiable information (PII) and / or personal health information (PHI). With the benefit of one embodiment of the present invention, healthcare related information could use TDRs that do not reveal sensitive PII/PHI without losing the context of, or access to, such information. Each successive level (starting with the provider level at the bottom and working up to the national level at the top) could be provided information in which PII/PHI information has been replaced with TDRs (comprised of dynamically changing and re-assignable DDIDs and the PII/PHI information) represented by temporally unique and purpose limited DDIDs only (without revealing the PII/PHI information) so sensitive PII/PHI data is not exposed. When access to PII/PHI information is necessary to perform an appropriate and authorized use at a specific level, association keys (AKs) and / or replacement keys (RKs) may be used to discern the relevant sensitive PII/PHI data associated with applicable TDRs and DDIDs. In addition, DDIDs could help facilitate self-regulation to improve longitudinal studies since DDIDs change over time and information associated with new DDIDs can reflect new and additional information without revealing the identity of a Data Subject/patient. This could be accomplished by using DDIDs to separate "context" or "meta" from the data necessary to perform analysis. The results of the analysis could be shared with a trusted party / proxy who would apply the "context" or "meta" to the data resulting from the analysis. There are a multitude of players in the healthcare industry - many of which use different data structures. Dynamic Anonymity could support collection of disparate data from different sources in different formats, normalize the information into a common structure and separate "context" or "meta" from "content" by means of dynamically assigning, reassigning and tracking DDIDs to enable effective research and analysis without revealing identifying information. This methodology could allow the linking of data together about a single Data Subject/patient from disparate sources without having to worry about getting consent because individuals would not be identifiable as a result of the

process. Only within the Circle of Trust ("CoT") identified in Figure 1C-1 will identifying information be accessible by means of access to the mapping engine that correlates information to individuals. With appropriate oversight and regulation, trusted parties / proxies could offer controls via a Circle of Trust (CoT) to help reconcile tensions between identifiable and functional information. For example, currently in healthcare / life science research, significant "data minimization" efforts are undertaken to ensure that only the minimal amount of identifiable information is used in research because of potential risk to individuals of re-identification. With Dynamic Anonymity, much of the burden placed on regulators regarding enforcement of laws and the burden on companies associated with privacy / anonymity reviews and engineering could be substantially reduced while at the same time, more complete data sets could be made available for healthcare-related research and development. HIPAA sets forth methodologies for de-identifying personal health information (PHI); once PHI is de-identified, it is no longer subject to HIPAA regulations and can be used for any purpose. However, concerns have been raised about the sufficiency of existing HIPAA de-identification methodologies, the lack of legal accountability for unauthorized re-identification of de-identified data, and insufficient public transparency about de-identified data uses. In addition, effective as of September 22, 2014 under the HIPAA / HITECH final rule, in addition to covered entities, business associates are also directly liable for HIPAA compliance. The present invention provides a means of accomplishing the information privacy objectives of HIPAA without diminishing the value of information. By means of application of the present invention, most data may be HIPAA compliant.

[0367] Figure 26 illustrates some potential benefits of an embodiment of the present disclosure in the area of mobile / wearable / portable device communications. Mobile/wearable/portable applications implementing a system or aspects thereof as disclosed herein, may provide the controlling entity control over both the timing and level of participation in location and time sensitive applications. The controlling entity may use the capabilities of the abstraction module of the privacy server to control the degree to which attribute combinations are shared with third parties, doing so in an anonymous versus personally identifiable manner. For example, static identifiers associated with a mobile / wearable / portable device in existing systems may enable mobile / wearable / portable application providers and other third parties to aggregate attribute combination data pertaining to use of the mobile / wearable / portable device. Use of the present invention may prevent application providers and other third parties from aggregating attribute combinations pertaining to use of a mobile / wearable / portable device and may further enable a mobile / wearable / portable device to use mobile applications requiring access to geolocation information (e.g., direction or map applications) without revealing the identity of the mobile / wearable / portable device or user by implementing the use of TDRs and / or DDIDs rather than static identifiers.

[0368] Figure 27 is an example of a simplified functional block diagram illustrating a programmable device 2700 according to one embodiment that can implement one or more of the processes, methods, steps, features or aspects described herein. The programmable device 2700 may include one or more communications circuitry 2710, memory 2720, storage device 2730, processor 2740, controlling entity interface 2750, display 2760, and communications bus 2770. Processor 2740 may be any suitable programmable control device or other processing unit, and may control the operation of many functions performed by programmable device 2700. Processor 2740 may drive display 2760 and may receive controlling entity inputs from the controlling entity interface 2750. An embedded processor provides a versatile and robust programmable control device that may be utilized for carrying out the disclosed techniques.

[0369] Storage device 2730 may store attribute combinations, software (e.g., for implementing various functions on device 2700), preference information, device profile information, and any other suitable data. Storage device 2730 may include one or more storage mediums for tangibly recording data and program instructions, including for example, a hard-drive or solid state memory, permanent memory such as ROM, semi-permanent memory such as RAM, or cache. Program instructions may comprise a software implementation encoded in any desired computer programming language.

[0370] Memory 2720 may include one or more different types of storage modules that may be used for performing device functions. For example, memory 2720 may include cache, ROM, and / or RAM. Communications bus 2770 may provide a data transfer path for transferring data to, from, or between at least memory 2720, storage device 2730, and processor 2740.

[0371] Although referred to as a bus, communications bus 2770 is not limited to any specific data transfer technology. Controlling entity interface 2750 may allow a controlling entity to interact with the programmable device 2700. For example, the controlling entity interface 2750 can take a variety of forms, such as a button, keypad, dial, click wheel, mouse, touch or voice command screen, or any other form of input or user interface.

[0372] In one embodiment, the programmable device 2700 may be a programmable device capable of processing data. For example, the programmable device 2600 may be a device such as any identifiable device (excluding smart phones, tablets, notebook and desktop computers) that have the ability to communicate and are embedded with sensors, identifying devices or machine-readable identifiers (a "smart device"), smart phone, tablet, notebook or desktop computer, or other suitable personal device.

[0373] Figure 28 is an example of a block diagram illustrating a system 2800 of networked devices for implementing one or more of the processes, methods, steps, features or aspects described herein. The privacy client described above may be implemented on any of the smart device (i.e., wearable, movable or immovable smart devices) 2810, smart

phone 2820, tablet 2830, notebook 2840, or desktop computer 2850, for example. Each of these devices is connected by one or more networks 2860 to the privacy server 2870, to which is coupled a database 2880 for storing information about attribute combinations, TDRs, Data Subjects, aggregated Data Subject profiles, time periods/stamps by means of time keys (TKs) or otherwise, association keys (AKs), replacement keys (RKs) and their associated information. The database 2880 may be any desired form of data storage, including structured databases and non-structured flat files. The privacy server 2870 may also provide remote storage for attribute combinations, TDRs, Data Subjects, aggregated Data Subject profiles, time periods/stamps by means of time keys (TKs) or otherwise, association keys (AKs), replacement keys (RKs) and their associated information that have been or are to be delivered to the privacy clients on devices 2810, 2820, 2830, 2840, 2850, or other suitable devices either in the database 2880 or in a different database (not shown).

[0374] Although a single network 2860 is illustrated in Figure 28, the network 2860 may be multiple interconnected networks, and the privacy server 2870 may be connected to each of the privacy clients on 2810, 2820, 2830, 2840, 2850, or other suitable devices via different networks 2860. The network 2860 may be any type of network, including local area networks, wide area networks, or the global internet.

[0375] Embodiments of the present invention can provide privacy and security applications for various industries, environments, and technologies, including, but not limited to, online transactions, healthcare, education, card payment or processing, information security, shipping, supply chain management, manufacturing resource planning, geolocation, mobile or cellular systems, energy and smart grid technologies, the internet, and the defense and intelligence technologies and programs.

[0376] When used in an online transaction environment, embodiments of the present invention can provide consumers with the ability to control collection or use of their data, and may provide data custodians the ability to ensure third parties involved in data communications or dissemination receive only information necessary for them to perform their specific function. The resulting increased consumer confidence may enable continued enjoyment of benefits of the "Internet of Things," as described above, without forsaking subject or related party rights or subjecting the industry to undue regulation.

[0377] In the healthcare field, embodiments of the present invention can help retain the efficacy of existing healthcare laws by improving de-identification. In addition, embodiments of the present invention may enable individual consumers and society as a whole to benefit from healthcare big data analytics by improving likelihood of patient consent for research due to increased protection of confidentiality of data.

[0378] As another example, when used in educational environments, embodiments of the present invention can provide educators and administrators with secure tools to access and use compartmentalized student-related data to enable students individually, and school systems collectively, to benefit from enhanced data analytics without jeopardizing students' rights to privacy / anonymity.

[0379] In the field of national security setting, an example embodiment of the invention may be used for instance by a governmental national security organization to analyze limited telephone records aggregated by individual telecommunications users, without requiring that any personally identifiable information be provided to the security organization. For example, the time of calls, the 'called to' and 'called from" number, the duration of calls and the zip code of the "called to" and "called from" numbers could be disclosed without having to expose telephone numbers making or receiving calls or personal information pertaining to calling or receiving parties. In this example, the security organization may analyze the limited telephone records to determine if any suspicious activity occurred at which point a warrant or other judicial approval may be issued to receive additional, more detailed attributes of the telephone records. In this manner, embodiments of the present invention can be used to further national security interests while at the same time maintaining the privacy / anonymity of telephone users until such time as a judicial review requires the disclosure of additional, more detailed attributes.

[0380] While the methods disclosed herein have been described and shown with reference to particular operations performed in a particular order, it will be understood that these operations may be combined, sub-divided, or reordered without departing from the teachings of the present invention. Accordingly, unless specifically indicated herein, the order and grouping of the operations is not a limitation of the present invention. For instance as a non-limiting example, in alternative embodiments, portions of operations described herein may be re-arranged and performed in different order than as described herein.

[0381] It should be appreciated that reference throughout this specification to "one embodiment" or "an embodiment" or "one example" or "an example" means that a particular feature, structure or characteristic described in connection with the embodiment may be included, if desired, in at least one embodiment of the present invention. Therefore, it should be appreciated that two or more references to "an embodiment" or "one embodiment" or "an alternative embodiment" or "one example" or "an example" in various portions of this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures or characteristics may be combined as desired in one or more embodiments of the invention.

[0382] It should be appreciated that in the foregoing description of exemplary embodiments of the invention, various features of the invention are sometimes grouped together in a single embodiment, figure, or description thereof for the purpose of streamlining the disclosure and aiding in the understanding of one or more of the various inventive aspects.

This method of disclosure, however, is not to be interpreted as reflecting an intention that the claimed inventions require more features than are expressly recited in each claim. Rather, inventive aspects lie in less than all features of a single foregoing disclosed embodiment, and each embodiment described herein may contain more than one inventive feature.

[0383] While the invention has been particularly shown and described with reference to embodiments thereof, it will be understood by those skilled in the art that various other changes in the form and details may be made without departing from the scope of the invention.

Claims

1. A system (2800) for anonymizing data subjects, comprising:

a communication interface for sending data over a network (2860);
a memory (2720) having, stored therein, computer program code; and
one or more processing units (2740) operatively coupled to the memory (2720), wherein the one or more processing units (2740) are configured to execute instructions in the computer program code that cause the one or more processing units (2740) to:

generate two or more different dynamically-changing, temporally unique identifiers;
receive, over the network (2860), a first request from a first client for generated identifiers of the two or more dynamically-changing, temporally unique identifiers related to a first data subject;
associate, in response to the first request, a first generated identifier of the two or more dynamically-changing, temporally unique identifiers with the first data subject;
generate first time period data, wherein the first time period data comprises information defining a first time period during which the first generated identifier is used to identify the first data subject;
generate second time period data, wherein the second time period data comprises information defining a second time period which is different to and non-overlapping with the first time period, during which the first generated identifier is used to identify a second data subject different from the first data subject, and during which the first generated identifier is not used to identify the first data subject;
associate, in response to the first request, a second generated identifier of the two or more dynamically-changing, temporally unique identifiers with the first data subject;
generate third time period data, wherein the third time period data comprises information defining a third time period which is different to and non-overlapping with the first time period during which the second generated identifier is used to identify the first data subject;

store, in the memory (2720), the first generated identifier, the second generated identifier, the first time period data, the second time period data, and the third time period data; and
send the first generated identifier and the second generated identifier over the network (2860) to the first client.

2. The system (2800) of claim 1, wherein the instructions in the computer program code further cause the one or more processing units (2740) to:
associate one or more data attributes with the first generated identifier.

3. The system (2800) of claim 2, wherein at least one of the one or more data attributes associated with the first generated identifier relates to an action, activity, process, purpose, identity, or trait of the first data subject.

4. The system (2800) of claim 3, wherein the instructions in the computer program code further cause the one or more processing units (2740) to:

receive, over the network (2860), a second request from a second client for at least one of the one or more data attributes associated with the first generated identifier during the first time period;
determine that the second request is authorized; and
grant, over the network (2860), the ability of second client to determine the requested one or more data attributes associated with the first generated identifier during the first time period.

5. The system (2800) of any preceding claim, wherein the instructions in the computer program code further cause the one or more processing units (2740) to:

associate one or more data attributes with the second generated identifier,
wherein at least one of the one or more data attributes associated with the second generated identifier relates to an action, activity, process, purpose, identity, or trait of the first data subject.

6. The system (2800) of claim 5, wherein at least one of the one or more data attributes associated with the first generated identifier is different from at least one of the one or more data attributes associated with the second generated identifier.

7. The system (2800) of any preceding claim, wherein the instructions in the computer program code further cause the one or more processing units (2740) to:

receive, over the network, from a second client, a second identifier related to a second data subject;
associate the second identifier with the second data subject;
generate fourth time period data, wherein the fourth time period data comprises information defining a fourth time period during which the second identifier may be used to identify the second data subject; and
store, in the memory, the second identifier and fourth time period data.

8. The system (2800) of claim 3, wherein the instructions in the computer program code further cause the one or more processing units (2740) to:
revoke, over the network (2860), the ability of the second client to determine the requested one or more data attributes associated with the first generated identifier during the second time period.

9. A non-transitory computer readable medium comprising computer executable instructions stored thereon for anonymizing data subjects, the computer executable instructions are operable to cause one or more processing units (2740) to:

generate two or more different dynamically-changing, temporally unique identifiers;
receive, over a network, a first request from a first client for generated identifiers of the two or more dynamically-changing, temporally unique identifiers related to a first data subject;
associate, in response to the first request, a first generated identifier of the two or more dynamically-changing, temporally unique identifiers with the first data subject;
generate first time period data, wherein the first time period data comprises information defining a first time period during which the first generated identifier is used to identify the first data subject;
generate second time period data, wherein the second time period data comprises information defining a second time period which is different to and non-overlapping with the first time period,
during which the first generated identifier is used to identify a second data subject different from the first data subject, and during which the first generated identifier is not used to identify the first data subject;
associate, in response to the first request, a second generated identifier of the two or more dynamically-changing, temporally unique identifiers with the first data subject;
generate third time period data, wherein the third time period data comprises information defining a third time period which is different to and non-overlapping with the first time period during which the second generated identifier is used to identify the first data subject;
store, in a memory (2720), the first generated identifier, the second generated identifier, the first time period data, the second time period data, and the third time period data; and
send the first generated identifier and the second generated identifier over the network to the first client.

10. The non-transitory computer readable medium of claim 9, wherein the instructions further cause the one or more processing units (2740) to:
associate one or more data attributes with the first generated identifier.

11. The non-transitory computer readable medium of claim 10, wherein at least one of the one or more data attributes associated with the first generated identifier relates to an action, activity, process, purpose, identity, or trait of the first data subject.

12. The non-transitory computer readable medium of claim 11, wherein the instructions further cause the one or more processing units (240) to:

receive, over the network (2860), a second request from a second client for at least one of the one or more data

attributes associated with the first generated identifier during the first time period;
determine that the second request is authorized; and
grant, over the network (2860), the ability of second client to determine the requested one or more data attributes associated with the first generated identifier during the first time period.

13. A method for anonymizing data subjects, comprising :

generating two or more different dynamically-changing, temporally unique identifiers;
receiving, over a network, a first request from a first client for generated identifiers of the two or more dynamically-changing, temporally unique identifiers related to a first data subject;
associating, in response to the first request, a first generated identifier of the two or more dynamically-changing, temporally unique identifiers with the first data subject;
generating first time period data, wherein the first time period data comprises information defining a first time period during which the first generated identifier is used to identify the first data subject;
generated second time period data, wherein the second time period data comprises information defining a second time period which is different to and non-overlapping with the first time period during which the first generated identifier is used to identify a second data subject different from the first data subject, and during which the first generated identifier is not used to identify the first data subject;
associate, in response to the first request, a second generated identifier of the two or more dynamically-changing, temporally unique identifiers with the first data subject;
generate third time period data, wherein the third time period data comprises information defining a third time period which is different to and non-overlapping with the first time period during which the second generated identifier is used to identify the first data subject;
storing, in a memory (2720), the first generated identifier, the second generated identifier, the first time period data, the second time period data, and the third time period data; and
sending the first generated identifier and the second generated identifier over the network to the first client.

Patentansprüche

1. System (2008) zur Anonymisierung von betroffenen Personen, umfassend:

eine Kommunikationsschnittstelle zum Senden von Daten über ein Netzwerk (2860),
einen Speicher (2720), in welchem ein Computerprogrammcode gespeichert ist; und
eine oder mehrere Verarbeitungseinheiten (2740), die mit dem Speicher betriebsmäßig verbunden sind, wobei die eine oder die mehreren Verarbeitungseinheiten (2740) konfiguriert sind für die Ausführung von Befehlen in dem Computerprogrammcode, welche die eine oder die mehreren Verarbeitungseinheiten (2740) veranlassen zum:

Erzeugen von zwei oder mehr verschiedenen sich dynamisch ändernden zeitlich eindeutigen Kennungen;
Empfangen, über das Netzwerk (2860), einer ersten Anforderung erzeugter Kennungen der zwei oder mehr sich dynamisch ändernden zeitlich eindeutigen Kennungen, die sich auf eine erste betroffene Person beziehen, von einem ersten Client;
Zuordnen einer ersten erzeugten Kennung der zwei oder mehr sich dynamisch ändernden zeitlich eindeutigen Kennungen zu der ersten betroffenen Person als Antwort auf die erste Anforderung;
Erzeugen von ersten Zeitraumdaten, wobei die ersten Zeitraumdaten Informationen enthalten, die einen ersten Zeitraum definieren, in welchem die erste erzeugte Kennung zur Identifizierung der ersten betroffenen Person verwendet wird;
Erzeugen von zweiten Zeitraumdaten, wobei die zweiten Zeitraumdaten Informationen enthalten, die einen sich von dem ersten Zeitraum unterscheidenden und sich mit dem erstem Zeitraum nicht überlappenden zweiten Zeitraum definieren, in welchem die erste erzeugte Kennung zur Identifizierung einer sich von der ersten betroffenen Person unterscheidenden zweiten betroffenen Person verwendet wird und in welchem die erste erzeugte Kennung nicht für die Identifizierung der ersten betroffenen Person verwendet wird;
Zuordnen einer zweiten erzeugten Kennung der zwei oder mehr sich dynamisch ändernden zeitlich eindeutigen Kennungen zu der ersten betroffenen Person als Antwort auf die erste Anforderung;
Erzeugen von dritten Zeitraumdaten, wobei die dritten Zeitraumdaten Informationen enthalten, die einen sich von dem ersten Zeitraum unterscheidenden und sich mit dem erstem Zeitraum nicht überlappenden dritten Zeitraum definieren, in welchem die zweite erzeugte Kennung zur Identifizierung der ersten betrof-

fenen Person verwendet wird;
Speichern der ersten erzeugten Kennung, der zweiten erzeugten Kennung, der ersten Zeitraumdaten, der zweiten Zeitraumdaten und der dritten Zeitraumdaten in dem Speicher (2720); und
Senden der ersten erzeugten Kennung und der zweiten erzeugten Kennung über das Netzwerk (2860) an den ersten Client.

2. System (2800) nach Anspruch 1, wobei die Befehle in dem Computerprogrammcode die eine oder die mehreren Verarbeitungseinheiten (2740) ferner veranlassen zum:
Zuordnen eines oder mehrere Datenattribute zu der ersten erzeugten Kennung.

3. System (2800) nach Anspruch 2, wobei sich mindestens eines des einen oder der mehreren Datenattribute, die der ersten erzeugten Kennung zugeordnet sind, auf eine Aktion, eine Aktivität, einen Vorgang, eine Absicht, eine Identität oder ein Merkmal der ersten betroffenen Person bezieht.

4. System (2800) nach Anspruch 3, wobei die Befehle in dem Computerprogrammcode die eine oder die mehreren Verarbeitungseinheiten (2740) ferner veranlassen zum:

Empfangen, über das Netzwerk (2860), einer zweiten Anforderung zumindest eines des einen oder der mehreren Datenattribute, die der ersten erzeugten Kennung zugeordnet sind, in dem ersten Zeitraum von einem zweiten Client;
Bestimmen, dass die zweite Anforderung autorisiert ist; und
Erteilen, über das Netzwerk (2860), der Berechtigung des zweiten Client, das angeforderte eine oder die angeforderten mehreren Datenattribute, die der ersten erzeugten Kennung zugeordnet sind, zu bestimmen in dem ersten Zeitraum.

5. System (2800) nach einem der vorhergehenden Ansprüche, wobei die Befehle in dem Computerprogrammcode die eine oder die mehreren Verarbeitungseinheiten (2740) ferner veranlassen zum:
Zuordnen eines oder mehrerer Datenattribute zu der zweiten erzeugten Kennung, wobei sich mindestens eines des einen oder der mehreren Datenattribute, die der zweiten erzeugten Kennung zugeordnet sind, auf eine Aktion, eine Aktivität, einen Vorgang, eine Absicht, eine Identität oder ein Merkmal der ersten betroffenen Person bezieht.

6. System (2800) nach Anspruch 5, wobei sich wenigstens eines des einen oder der mehreren Datenattribute, die der ersten erzeugten Kennung zugeordnet sind, von wenigstens einem des einen oder der mehreren Datenattribute unterscheidet, die der zweiten erzeugten Kennung zugeordnet sind.

7. System (2800) nach einem der vorhergehenden Ansprüche, wobei die Befehle in dem Computerprogrammcode die eine oder die mehreren Verarbeitungseinheiten (2740) veranlassen zum:

Empfangen, über das Netzwerk, einer sich auf eine zweite betroffene Person beziehenden zweiten Kennung von einem zweiten Client;
Zuordnen der zweiten Kennung zu der zweiten betroffenen Person;
Erzeugen von vierten Zeitraumdaten, wobei die vierten Zeitraumdaten Informationen enthalten, die einen vierten Zeitraum definieren, in welchem die zweite Kennung zur Identifizierung der zweiten betroffenen Person verwendet werden kann; und
Speichern der zweiten Kennung und der vierten Zeitraumdaten in dem Speicher.

8. System (2800) nach Anspruch 3, wobei die Befehle in dem Computerprogrammcode die eine oder die mehreren Verarbeitungseinheiten (2740) ferner veranlassen zum:
Widerrufen, über das Netzwerk (2860), der Berechtigung des zweiten Client zum Bestimmen des angeforderten einen oder der angeforderten mehreren Datenattribute, die der ersten erzeugten Kennung zugeordnet sind, in dem zweiten Zeitraum.

9. Nichttransitorisches computerlesbares Medium umfassend computerausführbare Befehle, die zum Anonymisieren von betroffenen Personen auf dem Medium gespeichert sind, wobei die computerausführbaren Befehle wirksam sind zum Veranlassen der einen oder der mehreren Dateneinheiten (2740) zum:

Erzeugen von zwei oder mehr verschiedenen sich dynamisch ändernden zeitlich eindeutigen Kennungen;
Empfangen, über ein Netzwerk, einer ersten Anforderung erzeugter Kennungen der zwei oder mehr sich dy-

namisch ändernden zeitlich eindeutigen Kennungen, die sich auf eine erste betroffene Person beziehen, von einem ersten Client;
Zuordnen einer ersten erzeugten Kennung der zwei oder mehr sich dynamisch ändernden zeitlich eindeutigen Kennungen zu der ersten betroffenen Person als Antwort auf die erste Anforderung;
Erzeugen von ersten Zeitraumdaten, wobei die ersten Zeitraumdaten Informationen enthalten, die einen ersten Zeitraum definieren, in welchem die erste erzeugte Kennung zur Identifizierung der ersten betroffenen Person verwendet wird;
Erzeugen von zweiten Zeitraumdaten, wobei die zweiten Zeitraumdaten Informationen enthalten, die einen sich von dem ersten Zeitraum unterscheidenden und sich mit dem erstem Zeitraum nicht überlappenden zweiten Zeitraum definieren, in welchem die erste erzeugte Kennung zur Identifizierung einer sich von der ersten betroffenen Person unterscheidenden zweiten betroffenen Person verwendet wird und in welchem die erste erzeugte Kennung nicht zur Identifizierung der ersten betroffenen Person verwendet wird;
Zuordnen einer zweiten erzeugten Kennung der zwei oder mehr sich dynamisch ändernden zeitlich eindeutigen Kennungen zu der ersten betroffenen Person als Antwort auf die erste Anforderung;
Erzeugen von dritten Zeitraumdaten, wobei die dritten Zeitraumdaten Informationen enthalten, die einen sich von dem ersten Zeitraum unterscheidenden und sich mit dem erstem Zeitraum nicht überlappenden dritten Zeitraum definieren, in welchem die zweite erzeugte Kennung zur Identifizierung der ersten betroffenen Person verwendet wird;
Speichern der ersten erzeugten Kennung, der zweiten erzeugten Kennung, der ersten Zeitraumdaten, der zweiten Zeitraumdaten und der dritten Zeitraumdaten in einem Speicher (2720); und
Senden der ersten erzeugten Kennung und der zweiten erzeugten Kennung über das Netzwerk an den ersten Client.

10. Nichttransitorisches computerlesbares Medium nach Anspruch 9, wobei die Befehle die eine oder die mehreren Verarbeitungseinheiten (2740) ferner veranlassen zum:
Zuordnen eines oder mehrerer Datenattribute zu der ersten erzeugten Kennung.

11. Nichttransitorisches computerlesbares Medium nach Anspruch 10, wobei sich mindestens eines des einen oder der mehreren Datenattribute, die der ersten erzeugten Kennung zugeordnet sind, auf eine Aktion, eine Aktivität, einen Vorgang, eine Absicht, eine Identität oder ein Merkmal der ersten betroffenen Person bezieht.

12. Nichttransitorisches computerlesbares Medium nach Anspruch 11, wobei die Befehle die eine oder die mehreren Verarbeitungseinheiten (240) ferner veranlassen zum:

Empfangen einer zweiten Anforderung zumindest eines des einen oder der mehreren Datenattribute, die der ersten erzeugten Kennung zugeordnet sind, in dem ersten Zeitraum von einem zweiten Client über das Netzwerk (2860);
Bestimmen, dass die zweite Anforderung autorisiert ist; und
Erteilen der Berechtigung des zweiten Client, das angeforderte eine oder die angeforderten mehreren Datenattribute, die der ersten erzeugten Kennung zugeordnet sind, zu bestimmen, in dem ersten Zeitraum über das Netzwerk (2860).

13. Verfahren zum Anonymisieren von betroffenen Personen, umfassend:

das Erzeugen von zwei oder mehr verschiedenen sich dynamisch ändernden zeitlich eindeutigen Kennungen;
das Empfangen, über ein Netzwerk, einer ersten Anforderung erzeugter Kennungen der zwei oder mehr sich dynamisch ändernden zeitlich eindeutigen Kennungen, die sich auf die erste betroffene Person beziehen, von einem ersten Client;
das Zuordnen einer ersten erzeugten Kennung der zwei oder mehr sich dynamisch ändernden zeitlich eindeutigen Kennungen zu der ersten betroffenen Person als Antwort auf die erste Anforderung;
das Erzeugen von ersten Zeitraumdaten, wobei die ersten Zeitraumdaten Informationen enthalten, die einen ersten Zeitraum definieren, in welchem die erste erzeugte Kennung zur Identifizierung der ersten betroffenen Person verwendet wird;
das Erzeugen von zweiten Zeitraumdaten, wobei die zweiten Zeitraumdaten Informationen enthalten, die einen sich von dem ersten Zeitraum unterscheidenden und sich mit dem ersten Zeitraum nicht überlappenden zweiten Zeitraum definieren, in welchem die erste erzeugte Kennung zur Identifizierung einer sich von der ersten betroffenen Person unterscheidenden zweiten betroffenen Person verwendet wird und in welchem die erste erzeugte Kennung nicht zur Identifizierung der ersten betroffenen Person verwendet wird;

das Zuordnen einer zweiten erzeugten Kennung der zwei oder mehr sich dynamisch ändernden zeitlich eindeutigen Kennungen zu der ersten betroffenen Person als Antwort auf die erste Anforderung;
das Erzeugen von dritten Zeitraumdaten, wobei die dritten Zeitraumdaten Informationen enthalten, die einen sich von dem ersten Zeitraum unterscheidenden und sich mit dem ersten Zeitraum nicht überlappenden dritten Zeitraum definieren, in welchem die zweite erzeugte Kennung zur Identifizierung der ersten betroffenen Person verwendet wird;
das Speichern der ersten erzeugten Kennung, der zweiten erzeugten Kennung, der ersten Zeitraumdaten, der zweiten Zeitraumdaten und der dritten Zeitraumdaten in einem Speicher (2720); und
das Senden der ersten erzeugten Kennung und der zweiten erzeugten Kennung über das Netzwerk an den Client.

Revendications

1. Système (2800) permettant l'anonymisation de personnes concernées comprenant :

une interface de communication permettant de transmettre des données sur un réseau (2860),
une mémoire (2720) dans laquelle est stocké un code-programme d'ordinateur, et
au moins une unité de traitement (2740) fonctionnellement couplée à la mémoire (2720),
dans lequel la ou les unité(s) de traitement (2740) est(sont) conformée(s) pour exécuter des instructions renfermées dans le code-programme d'ordinateur qui commandent la ou les unité(s) de traitement (2740) pour :

créer deux ou un plus grand nombre d'identifiants différents à modification dynamique temporellement uniques,
recevoir sur le réseau (2860) une première demande provenant d'un premier client des identifiants créés parmi les deux ou le plus grand nombre d'identifiants à modification dynamique temporellement uniques relatifs à une première personne concernée,
associer en réponse à la première demande un premier identifiant créé parmi les deux ou le plus grand nombre d'identifications à modification dynamique temporellement uniques, à la première personne concernée,
créer des données de premières période de temps, les premières données de période de temps renfermant une information définissant une première période de temps au cours de laquelle le premier identifiant créé est utilisé pour identifier la première personne concernée,
créer des secondes données de période de temps, les secondes données de période de temps renfermant une information définissant une seconde période de temps qui est différente de la première période de temps et ne chevauche pas celle-ci au cours de laquelle le premier identifiant créé est utilisé pour identifier une seconde personne concernée différente de la première personne concernée et au cours de laquelle le premier identifiant créé n'est pas utilisé pour identifier la première personne concernée,
associer en réponse à la première demande un second identifiant créé parmi les deux ou le plus grand nombre d'identifiants à modification dynamique temporellement uniques à la première personne concernée,
créer des troisièmes données de période de temps, les troisièmes données de période de temps renfermant une information définissant une troisième période de temps qui est différente de la première période de temps et ne chevauche pas celle-ci au cours de laquelle le second identifiant créé est utilisé pour identifier la première personne concernée,
stocker dans la mémoire (2720) le premier identifiant créé, le second identifiant créé, les premières données de période de temps, les secondes données de période de temps et les troisièmes données de période de temps, et
transmettre le premier identifiant créé et le second identifiant créé sur le réseau (2860) au premier client.

2. Système (2800) conforme à la revendication 1,
dans lequel les instructions renfermées dans le code programme d'ordinateur commandent en outre la ou les unité(s) de traitement (2740) pour associer un ou plusieurs attribut(s) de données au premier identifiant créé.

3. Système (2800) conforme à la revendication 2,
dans lequel au moins un attribut de données associé au premier identifiant créé est relatif à une action, une activité, un procédé, un but, l'identité ou un caractère de la première personne concernée.

4. Système (2800) conforme à la revendication 3,

dans lequel les instructions renfermées dans le code programme d'ordinateur commandent en outre la ou les unité(s) de traitement (2740) pour :

recevoir sur le réseau (2860) une seconde demande provenant d'un second client d'au moins un attribut de données associé au premier identifiant créé au cours de la première période de temps,
déterminer que la seconde demande est autorisée, et
accorder sur le réseau (2860) l'aptitude du second client pour déterminer le ou les attributs de données demandés associés au premier identifiant créé pendant la première période de temps.

5. Système (2800) conforme à l'une quelconque des revendications précédentes,
dans lequel les instructions renfermées dans le code programme d'ordinateur commandent en outre la ou les unité(s) de traitement (2740) pour :

associer un ou plusieurs attribut(s) de données au second identifiant créé,
au moins l'un des attributs de données associé au second identifiant créé étant relatif à une action, une activité, un procédé, un but, l'identité ou un caractère de la première personne concernée.

6. Système (2800) conforme à la revendication 5,
dans lequel au moins l'un des attributs de données associé au premier identifiant créé est différent d'au moins l'un des attributs de données associé au second identifiant créé.

7. Système (2800) conforme à l'une quelconque des revendications précédentes,
dans lequel les instructions renfermées dans le code programme d'ordinateur commandent en outre la ou les unité(s) de traitement (2740) pour :

recevoir sur le réseau, à partir d'un second client, un second identifiant relatif à une seconde personne concernée,
associer le second identifiant à la seconde personne concernée,
créer des quatrièmes données de période de temps, les quatrièmes données de période de temps renfermant une information définissant une quatrième période de temps au cours de laquelle le second identifiant peut être utilisé pour identifier la seconde personne concernée, et
stocker dans la mémoire le second identifiant et les quatrièmes données de période de temps.

8. Système (2800) conforme à la revendication 3,
dans lequel les instructions renfermées dans le code programme d'ordinateur commandent en outre la ou les unité(s) de traitement (2740) pour :
supprimer sur le réseau (2860) l'aptitude du second client à déterminer le ou les attribut(s) de données demandée(s) associée(s) au premier identifiant créé pendant la seconde période de temps.

9. Support lisible par un ordinateur non transitoire comprenant :

des instructions exécutables par ordinateur stockées dans celui-ci pour permettre l'anonymisation de personnes concernées,
les instructions exécutables par ordinateur pouvant être mises en œuvre pour commander une ou plusieurs unité(s) de traitement (2740) pour :

créer deux ou un plus grand nombre d'identifiants différents à modification dynamique temporellement uniques,
recevoir sur un réseau une première demande provenant d'un premier client pour des identifiants créés parmi les deux ou le plus grand nombre d'identifiants à modification dynamique temporellement uniques relatifs à une première personne concernée,
associer en réponse à la première demande un premier identifiant créé parmi les deux ou le plus grand nombre d'identifiants à modification dynamique temporellement uniques à la première personne concernée,
créer des premières données de période de temps, les données de première période de temps renfermant une information définissant une première période de temps au cours de laquelle le premier identifiant créé est utilisé pour identifier la première personne concernée,
créer des secondes données de période de temps, les secondes données de période de temps renfermant une information définissant une seconde période de temps qui est différente de la première période de temps et ne se chevauche pas avec celle-ci, au cour de laquelle le premier identifiant créé est utilisé pour

identifier une seconde personne concernée différente de la première personne concernée et au cours de laquelle le premier identifiant créé n'est pas utilisé pour identifier la première personne concernée,
associer en réponse à la première demande, un second identifiant créé parmi les deux ou le plus grand nombre d'identifiants à modification dynamique temporellement uniques à la première personne concernée,
créer des troisièmes données de période de temps, les troisièmes données de période de temps renfermant une information définissant une troisième période de temps qui est différente de la première période de temps et ne se chevauche pas avec celle-ci pendant laquelle le second identifiant créé est utilisé pour identifier la première personne concernée,
stocker dans une mémoire (2720) le premier identifiant créé, le second identifiant créé, les premières données de période de temps, les secondes données de période de temps et les troisièmes données de période de temps, et
transmettre le premier identifiant créé et le second identifiant créé sur le réseau au premier client.

10. Support lisible par un ordinateur non transitoire conforme à la revendication 9,
dans lequel les instructions commandent en outre la ou les unités de traitement (2740) pour :
associer un ou plusieurs attributs de données avec le premier identifiant créé.

11. Support lisible par un ordinateur non transitoire conforme à la revendication 10,
dans lequel au moins un attribut de données associé au premier identifiant créé est relatif à une action, une activité, un procédé, un but, l'identité ou à un caractère de la première personne concernée.

12. Support lisible par un ordinateur non transitoire conforme à la revendication 11,
dans lequel les instructions commandent en outre la ou les unité(s) de traitement (240) pour :

recevoir sur le réseau (2860) une seconde demande provenant d'un second client pour au moins un attribut de données associé au premier identifiant créé pendant la première période de temps,
déterminer que la seconde demande est autorisée, et
accorder sur le réseau (2860) l'aptitude du second client pour déterminer le ou les attribut(s) de données demandés associée(s) avec le premier identifiant créé pendant la première période de temps.

13. Procédé permettant l'anonymisation de personnes concernées comprenant des étapes consistant à :

créer deux ou un plus grand nombre d'identifiants différents à modification dynamique temporellement uniques,
recevoir sur un réseau une première demande provenant d'un premier client pour des identifiants créés parmi les deux ou le plus grand nombre d'identifiants à modification dynamique temporellement uniques relatifs à une première personne concernée,
associer en réponse à la première demande un premier identifiant créé parmi les deux ou le plus grand nombre d'identifiants à modification dynamique temporellement uniques à la première personne concernée,
créer des premières données de période de temps, les premières données de période de temps renfermant une information définissant une première période de temps au cours de laquelle le premier identifiant créé est utilisé pour identifier la première personne concernée,
créer des secondes données de période de temps, les secondes données de période de temps renfermant une information définissant une seconde période de temps qui est différente de la première période de temps et ne se chevauche pas avec celle-ci au cours de laquelle le premier identifiant créé est utilisé pour identifier une seconde personne concernée différente de la première personne concernée et au cours de laquelle le premier identifiant créé n'est pas utilisé pour identifier la première personne concernée,
associer en réponse à la première demande, un second identifiant créé parmi les deux ou le plus grand nombre d'identifiants à modification dynamique temporellement uniques à la première personne concernée,
créer des troisièmes données de période de temps, les troisièmes données de période de temps renfermant une information définissant une troisième période de temps qui est différente de la première période de temps et ne se chevauche pas avec celle-ci au cours de laquelle le second identifiant créé est utilisé pour identifier la première personne concernée,
stocker dans une mémoire (2720) le premier identifiant créé, le second identifiant créé, les premières données de période de temps, les secondes données de période de temps et les troisièmes données de période de temps, et
transmettre le premier identifiant créé et le second identifiant créé sur le réseau au premier client.

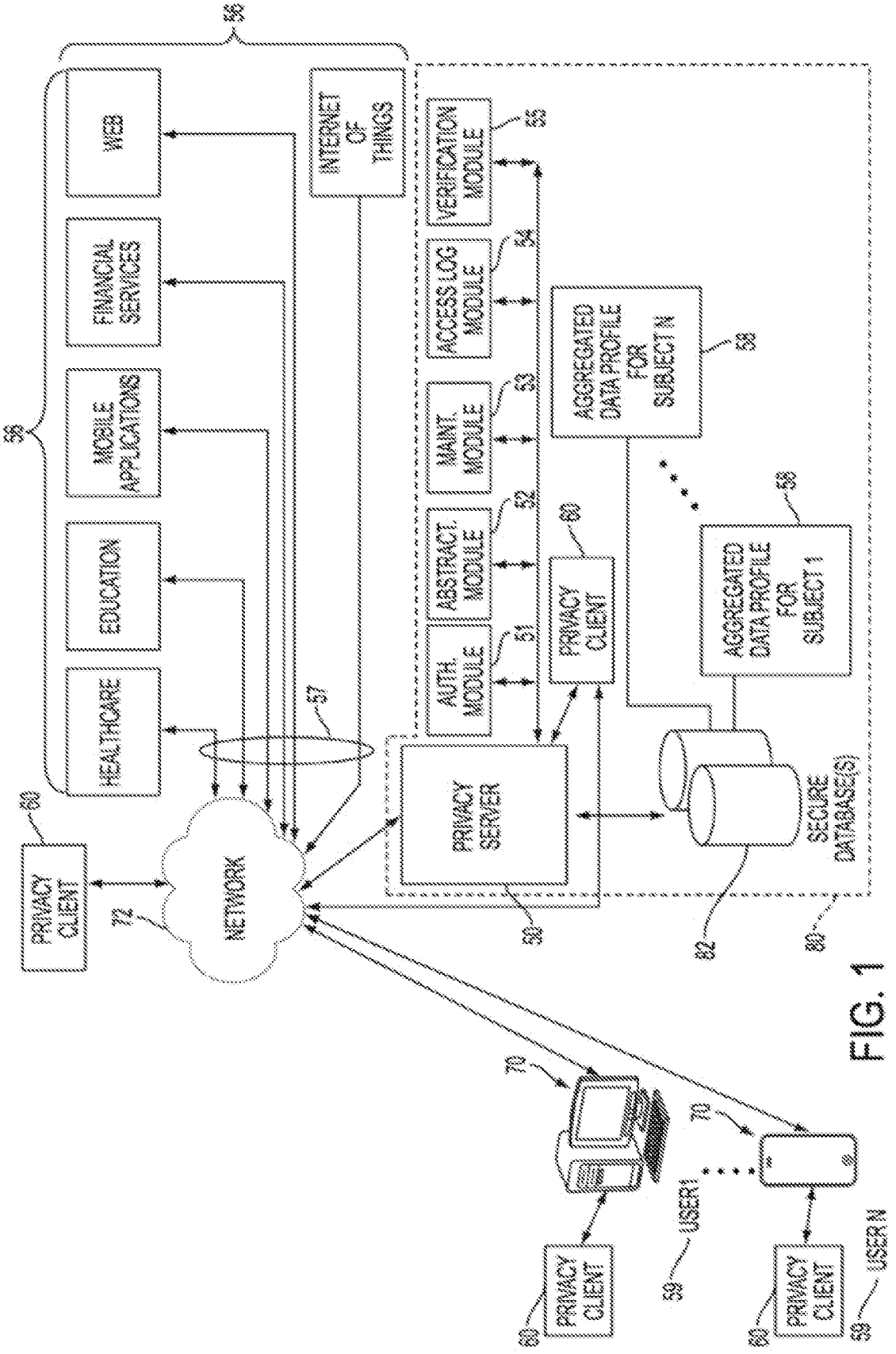

56
WEB
FINANCIAL SERVICES
MOBILE APPLICATIONS
EDUCATION
HEALTHCARE
INTERNET OF THINGS
VERIFICATION MODULE
55
ACCESS LOG MODULE
54
MAINT. MODULE
53
ABSTRACT MODULE
52
AUTH. MODULE
51
AGGREGATED DATA PROFILE FOR SUBJECT N
58
AGGREGATED DATA PROFILE FOR SUBJECT 1
58
PRIVACY CLIENT
60
PRIVACY SERVER
50
SECURE DATABASE(S)
82
80
NETWORK
72
57
70
USER1
59
USER N
59

FIG. 1

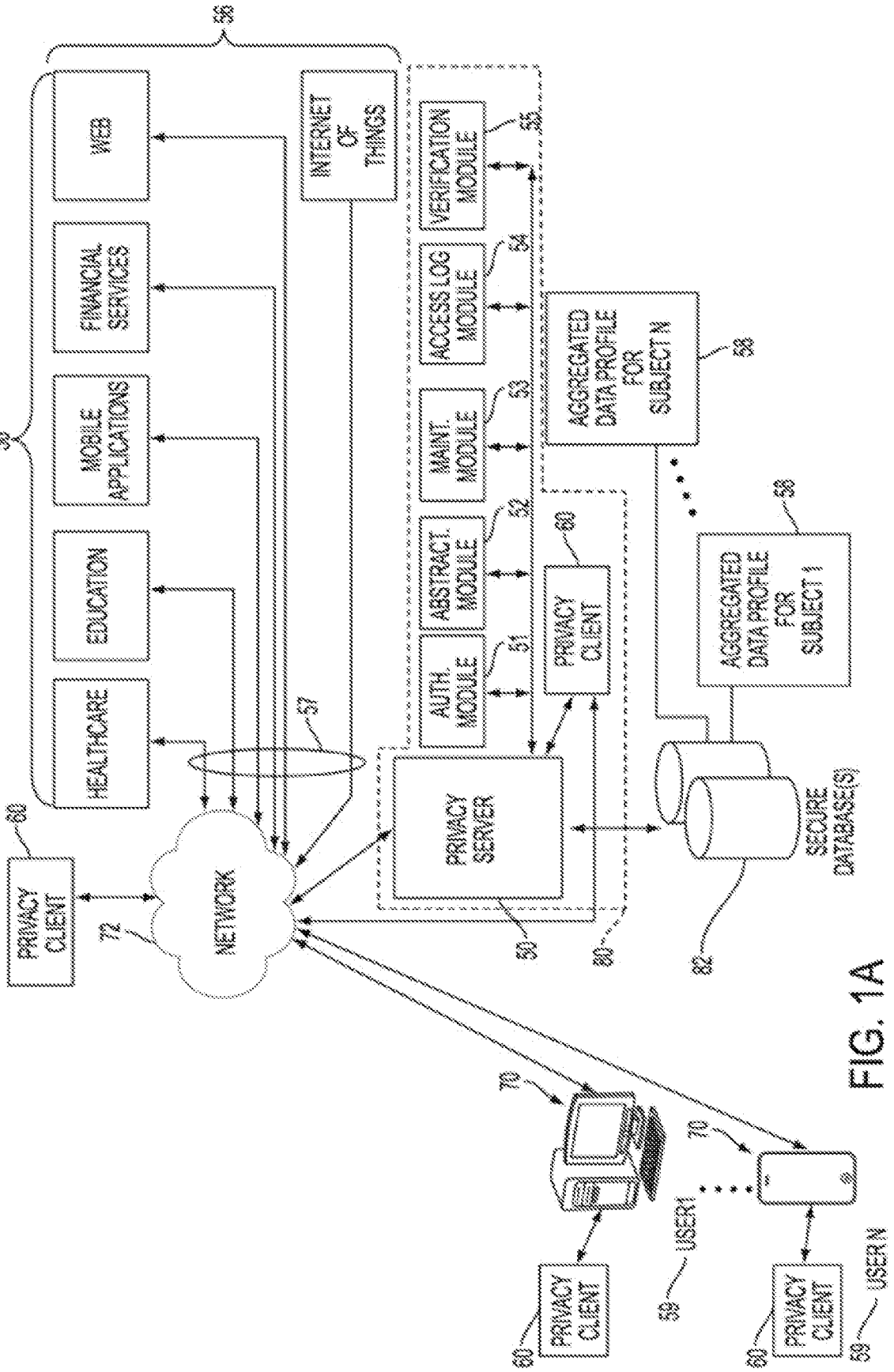

55
WEB
FINANCIAL SERVICES
MOBILE APPLICATIONS
EDUCATION
HEALTHCARE
INTERNET OF THINGS
VERIFICATION MODULE
ACCESS LOG MODULE
MAINT. MODULE
ABSTRACT. MODULE
AUTH. MODULE
AGGREGATED DATA PROFILE FOR SUBJECT N
AGGREGATED DATA PROFILE FOR SUBJECT 1
PRIVACY CLIENT
PRIVACY SERVER
SECURE DATABASE(S)
NETWORK
USER 1
USER N
50
51
52
53
54
56
57
58
59
60
70
72
80
82

FIG. 1A

FIG. 1B

ASSIGNMENT, APPLICATION, EXPIRATION AND RECYCLING OF DDIDS WITH RESPECT TO DATA ATTRIBUTES AND/OR ATTRIBUTE COMBINATIONS MAY OCCUR IN ANY OF THE FOLLOWING, OR COMBINATION OF THE FOLLOWING, WAYS:

1.PURPOSE BASED	2 PHYSICAL LOCATION BASED	3.VIRTUAL LOCATION BASED	4 TEMPORALLY BASED
A . BROWSE	A. ENTER	A. ENTER	A. RANDOM
B. DATA SUBJECT	B. EXIT	B. EXIT	B. SET
C. TRANSACTION	C. CHANGE	C. CHANGE	C. INTERVAL
D. OTHER	D. GENERAL	D. PAGE	D. OTHER
	E. SPECIFIC	E. SITE	
	F. OTHER	F. OTHER	

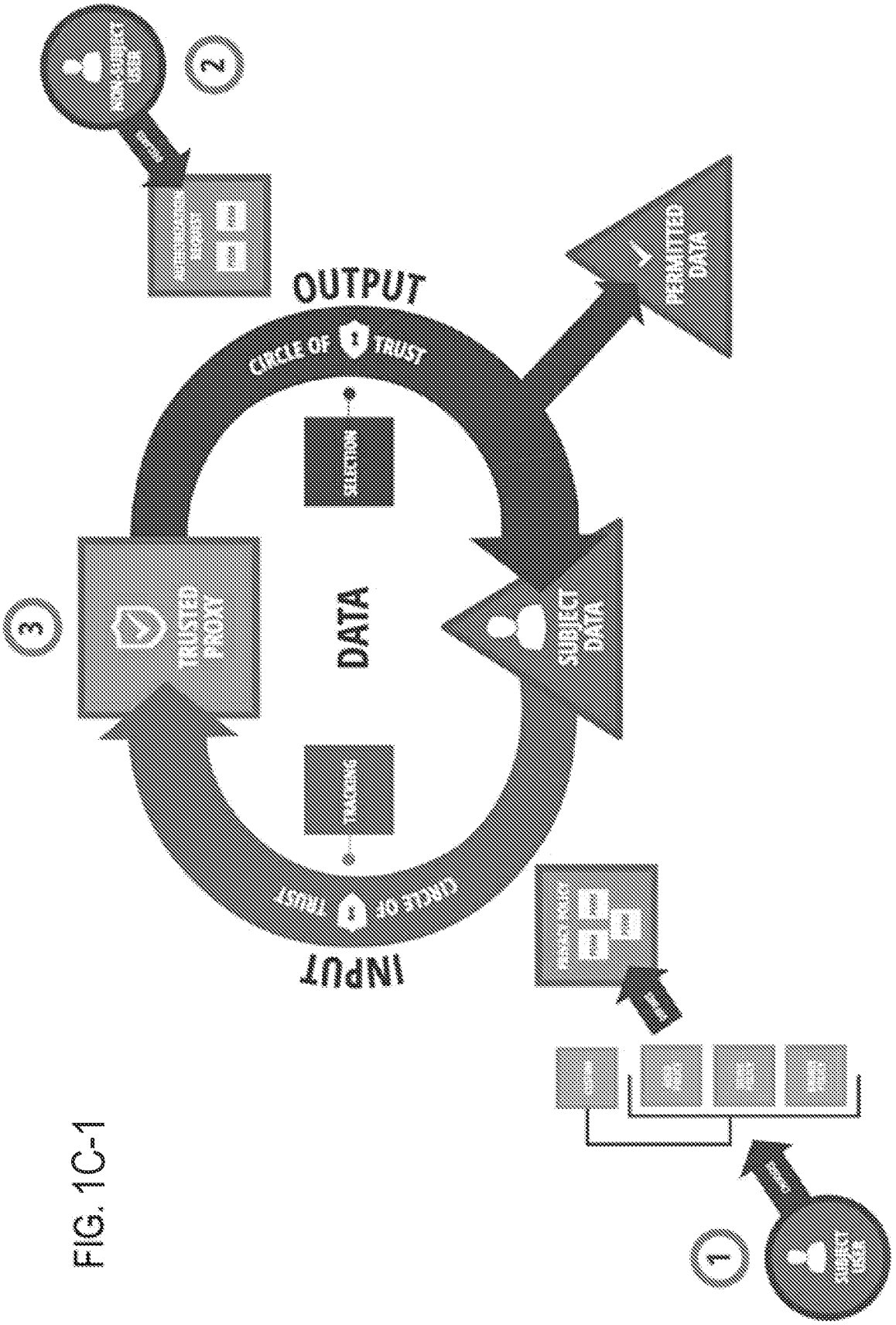
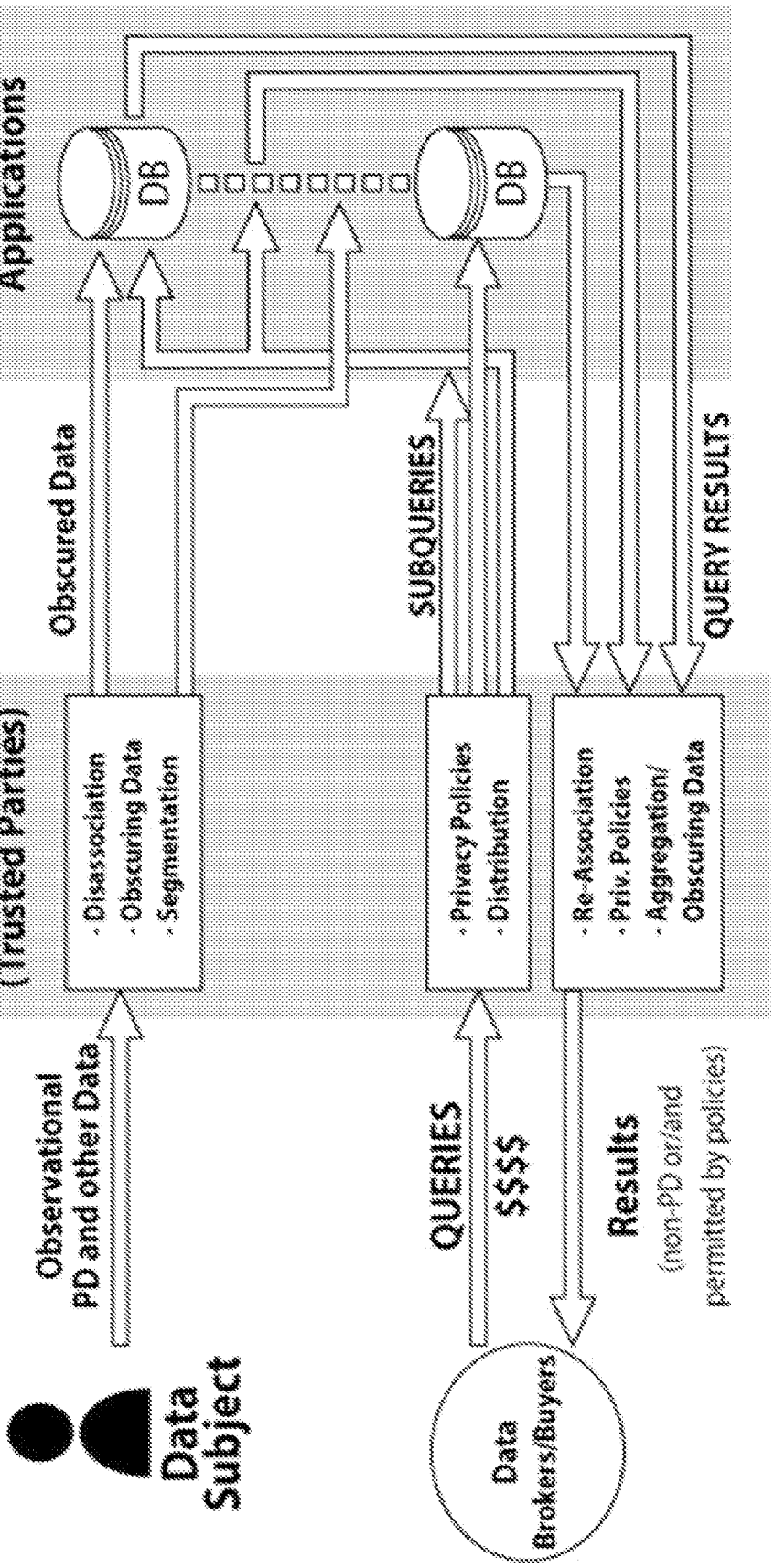

OUTPUT
CIRCLE OF TRUST
PERMITTED DATA
PROTECTION
TRUSTED PROXY
DATA
SUBJECT DATA
PROTECTION
CIRCLE OF TRUST
INPUT
SUBJECT DATA
SUBJECT USER
1
2
3

FIG. 1C-1

FIG. 1C-2


Third Parties/
Applications
DB
DB
Obscured Data
SUBQUERIES
QUERY RESULTS
Circle of Trust
(Trusted Parties)
· Disassociation
· Obscuring Data
· Segmentation
· Privacy Policies
· Distribution
· Re-Association
· Priv. Policies
· Aggregation/
Obscuring Data
Observational
PD and other Data
QUERIES
$$$$
Results
(non-PD or/and
permitted by policies)
Data Subject
Data
Brokers/Buyers

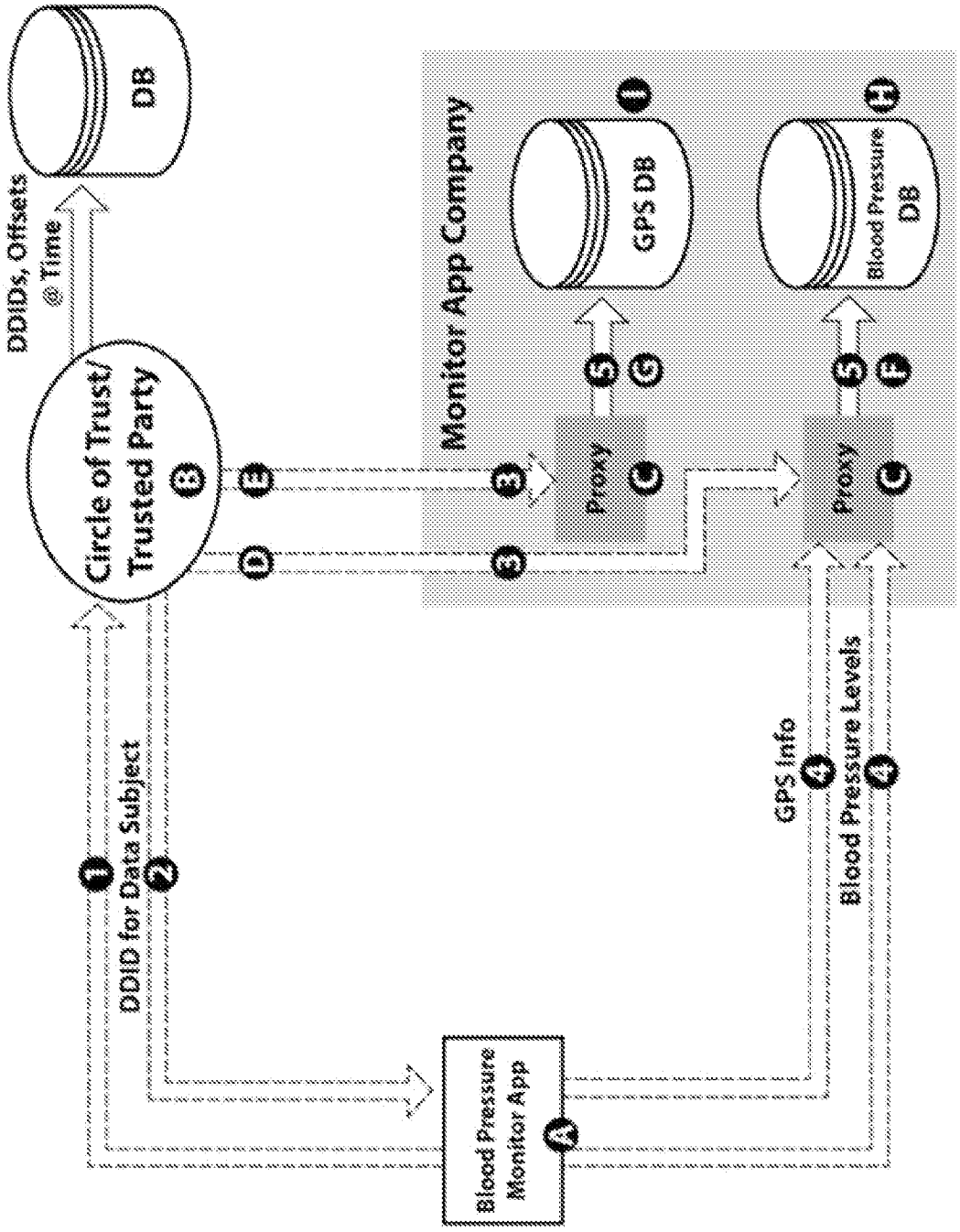

DB
DDIDs, Offsets
@ Time
Circle of Trust/
Trusted Party
Monitor App Company
GPS DB
Blood Pressure
DB
Proxy
Proxy
DDID for Data Subject
GPS Info
Blood Pressure Levels
Blood Pressure
Monitor App

FIG. 1D

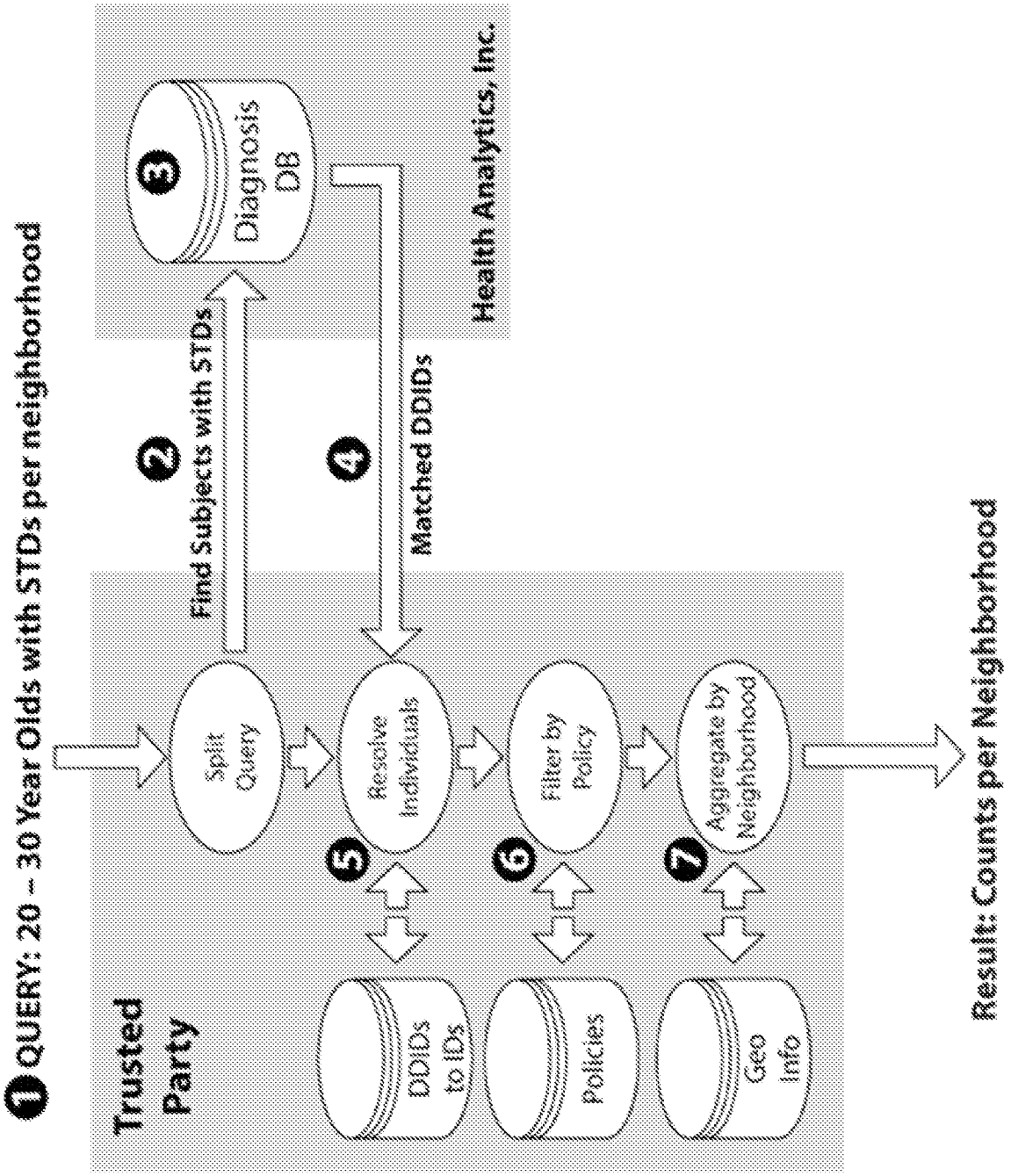

1 QUERY: 20 – 30 Year Olds with STDs per neighborhood
Trusted Party
Split Query
Resolve Individuals
Filter by Policy
Aggregate by Neighborhood
DDIDs to IDs
Policies
Geo Info
2 Find Subjects with STDs
3 Diagnosis DB
Health Analytics, Inc.
4 Matched DDIDs
5
6
7
Result: Counts per Neighborhood

FIG. 1E

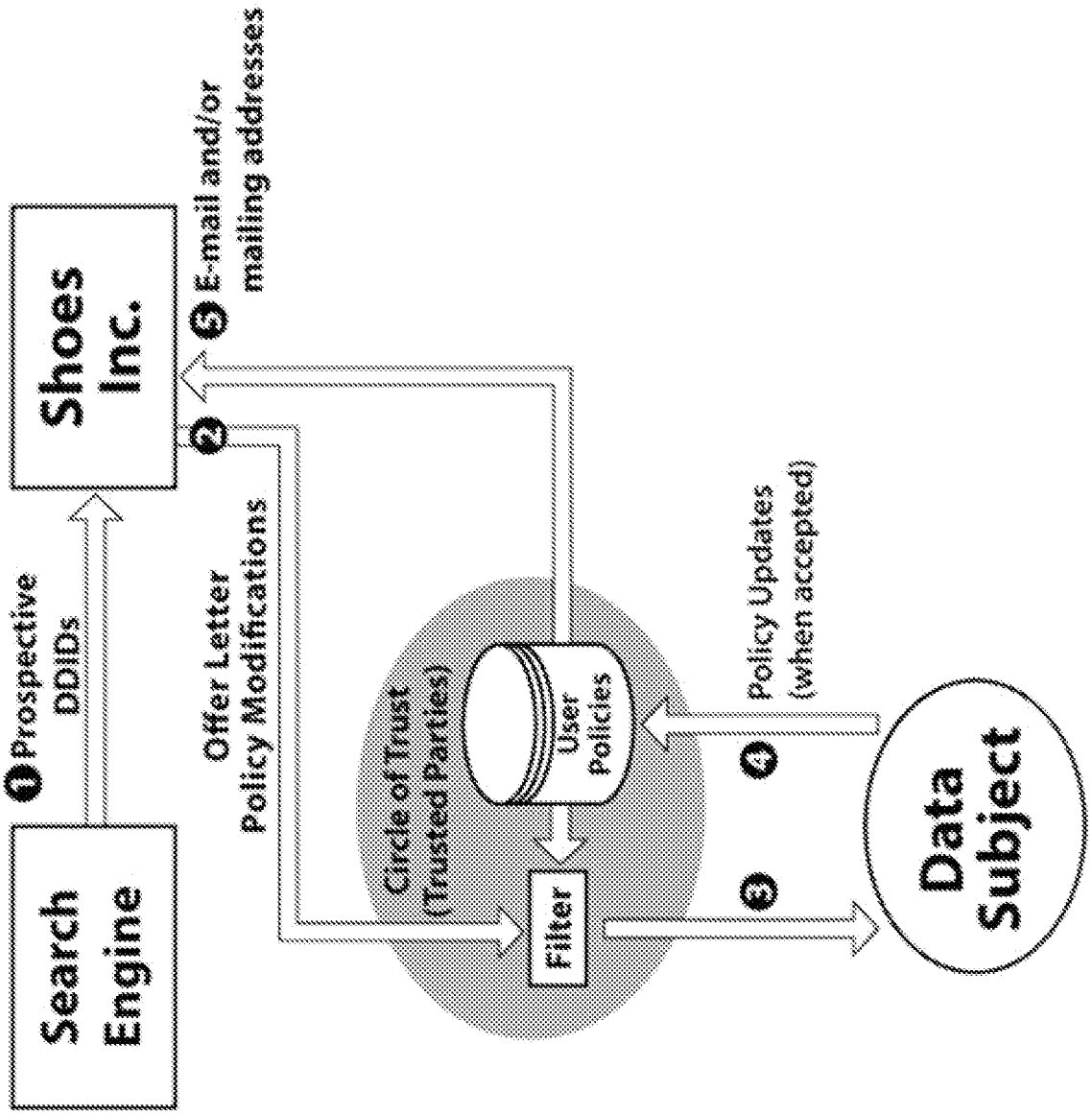

Search Engine
Shoes Inc.
1 Prospective DDIDs
2 E-mail and/or mailing addresses
Offer Letter
Policy Modifications
Circle of Trust (Trusted Parties)
User Policies
Filter
3
4 Policy Updates (when accepted)
Data Subject

FIG. 1F

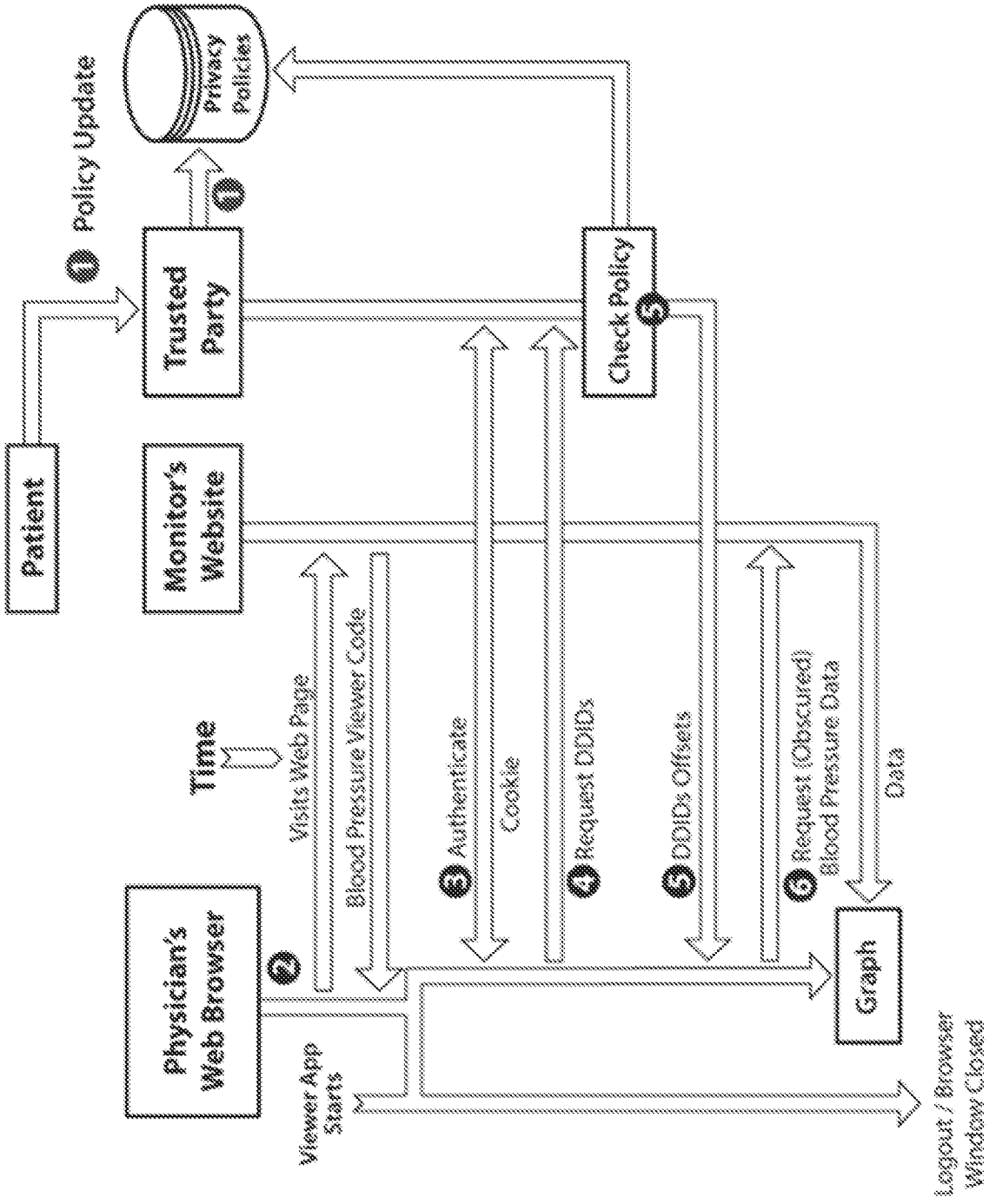

Privacy Policies
Policy Update
Trusted Party
Check Policy
Patient
Monitor's Website
Time
Visits Web Page
Blood Pressure Viewer Code
Authenticate
Cookie
Request DDIDs
DDIDs Offsets
Request (Obscured) Blood Pressure Data
Data
Physician's Web Browser
Graph
Viewer App Starts
Logout / Browser Window Closed

FIG. 1G

FIG. 1H

1H-A. Non-Obscured Data Elements

1H-B. Obscured Data Elements

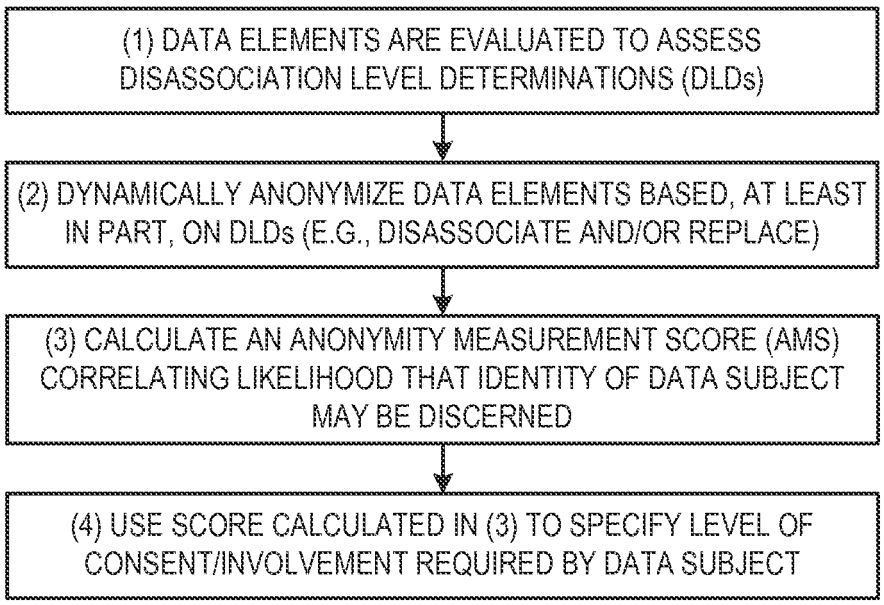

(1) DATA ELEMENTS ARE EVALUATED TO ASSESS DISASSOCIATION LEVEL DETERMINATIONS (DLDs)
(2) DYNAMICALLY ANONYMIZE DATA ELEMENTS BASED, AT LEAST IN PART, ON DLDs (E.G., DISASSOCIATE AND/OR REPLACE)
(3) CALCULATE AN ANONYMITY MEASUREMENT SCORE (AMS) CORRELATING LIKELIHOOD THAT IDENTITY OF DATA SUBJECT MAY BE DISCERNED
(4) USE SCORE CALCULATED IN (3) TO SPECIFY LEVEL OF CONSENT/INVOLVEMENT REQUIRED BY DATA SUBJECT

FIG. 1I

FIG. 1J

	Non-Disassociated /Replaced	Disassociation / Replacement Level 1	Disassociation / Replacement Level 2	Disassociation / Replacement Level 3
Social Security Number	100	90	81	40.5
Credit Card Number	75	67.5	60.75	30.375
First Name	25	22.5	20.25	10.125
Last Name	25	22.5	20.25	10.125
Birthdate	25	22.5	20.25	10.125
Age	20	18	16.2	8.1
Sex	10	9	8.1	4.05

Level 1 =

DDIDs are assigned for purposes of disassociation and/or replacement and retain their initially assigned value(s) – i.e., permanent assignments

Level 2 =

DDIDs are assigned for purposes of disassociation and/or replacement and retain their initially assigned value(s) until the value(s) are changed on an ad hoc basis – i.e., ad hoc changeability.

Level 3 =

DDIDs are assigned for purposes of disassociation and/or replacement and retain their initially assigned value(s) until the value(s) are changed based on a random, fixed, variable or other dynamic basis – i.e., dynamic changeability.

EP 3 063 691 B1

FIG. 1K

Category A = Aggregated score of 75+
Category B = Aggregated score of 40 to 74.9
Category C = Aggregated score of 39.9 and lower

Category A = Data set may be used only with current, express and unambiguous consent of data subject.

Category B = Data set may be used with (i) current or (ii) prior, express consent of data subject.

Category C = Data set may be used without requiring consent of data subject.

EP 3 063 691 B1

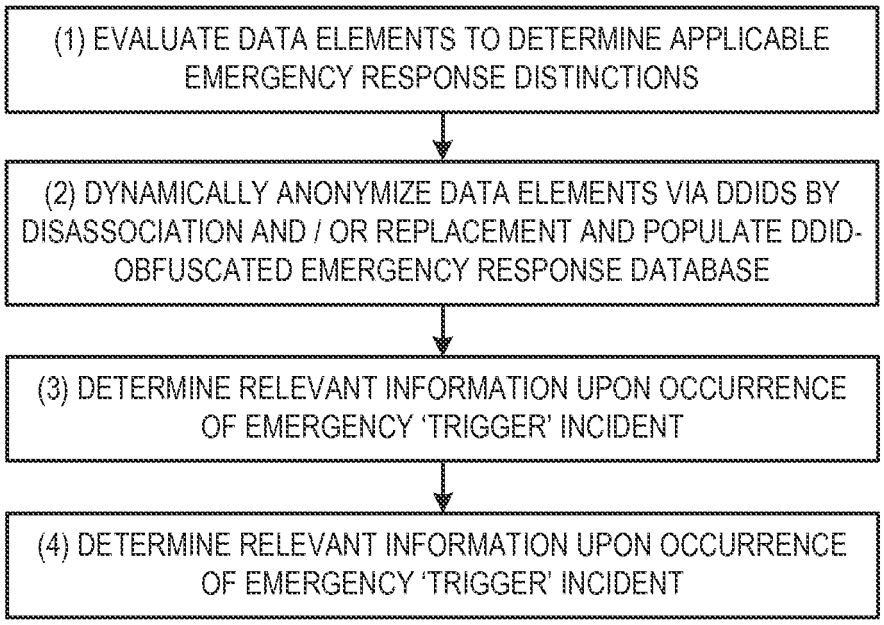

(1) EVALUATE DATA ELEMENTS TO DETERMINE APPLICABLE EMERGENCY RESPONSE DISTINCTIONS
(2) DYNAMICALLY ANONYMIZE DATA ELEMENTS VIA DDIDS BY DISASSOCIATION AND / OR REPLACEMENT AND POPULATE DDID-OBFUSCATED EMERGENCY RESPONSE DATABASE
(3) DETERMINE RELEVANT INFORMATION UPON OCCURRENCE OF EMERGENCY 'TRIGGER' INCIDENT
(4) DETERMINE RELEVANT INFORMATION UPON OCCURRENCE OF EMERGENCY 'TRIGGER' INCIDENT

FIG. 1L

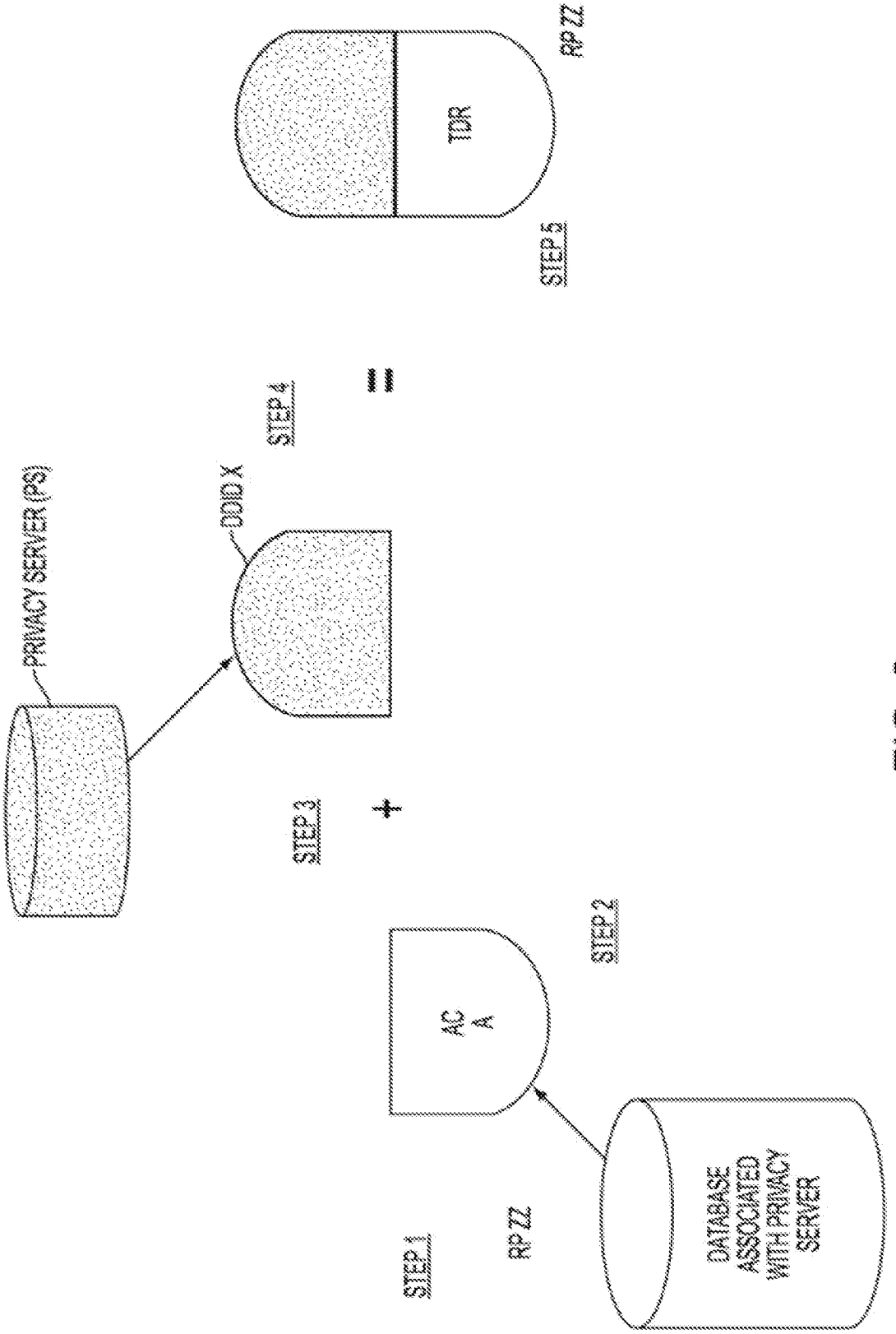

RP ZZ
TDR
STEP 5
=
STEP 4
DDID X
PRIVACY SERVER (PS)
+
STEP 3
STEP 2
AC
A
STEP 1
RP ZZ
DATABASE
ASSOCIATED
WITH PRIVACY
SERVER

FIG. 2

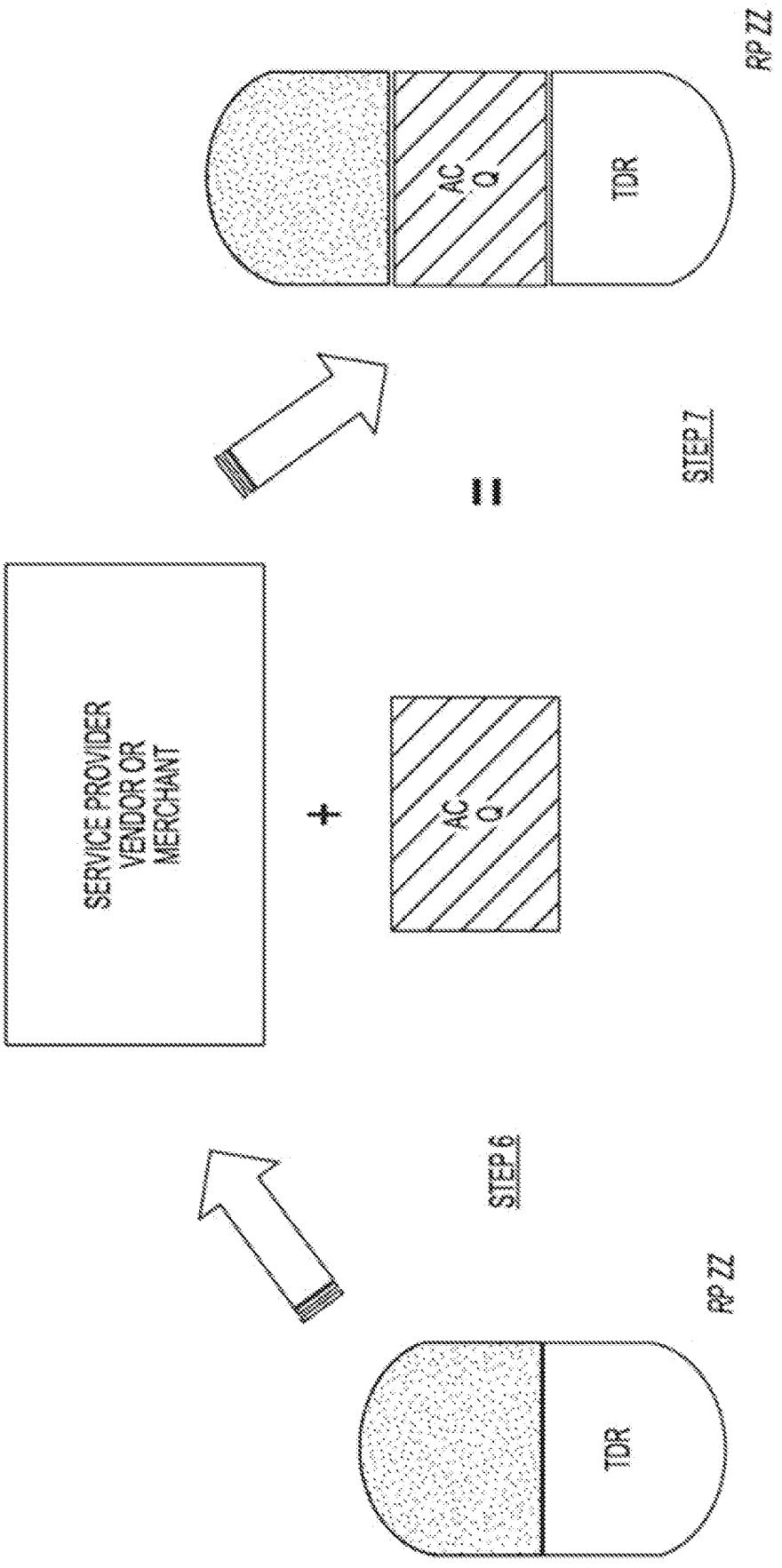

SERVICE PROVIDER
VENDOR OR
MERCHANT
+
AC
Q
=
AC
Q
TDR
RP ZZ
STEP 7
STEP 6
TDR
RP ZZ

FIG. 3

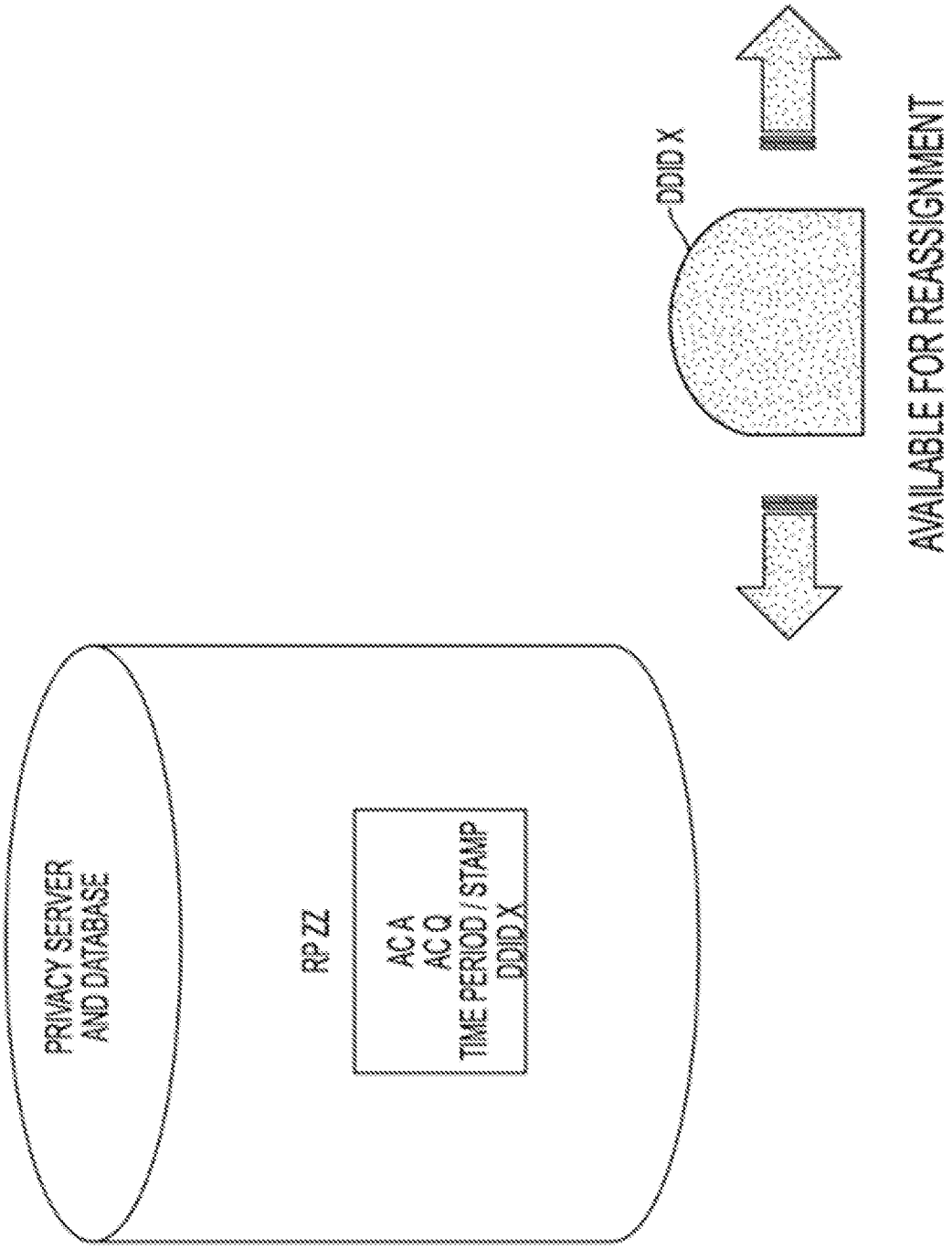

PRIVACY SERVER
AND DATABASE
RP ZZ
AC A
AC Q
TIME PERIOD / STAMP
DDID X
DDID X
AVAILABLE FOR REASSIGNMENT

FIG. 4

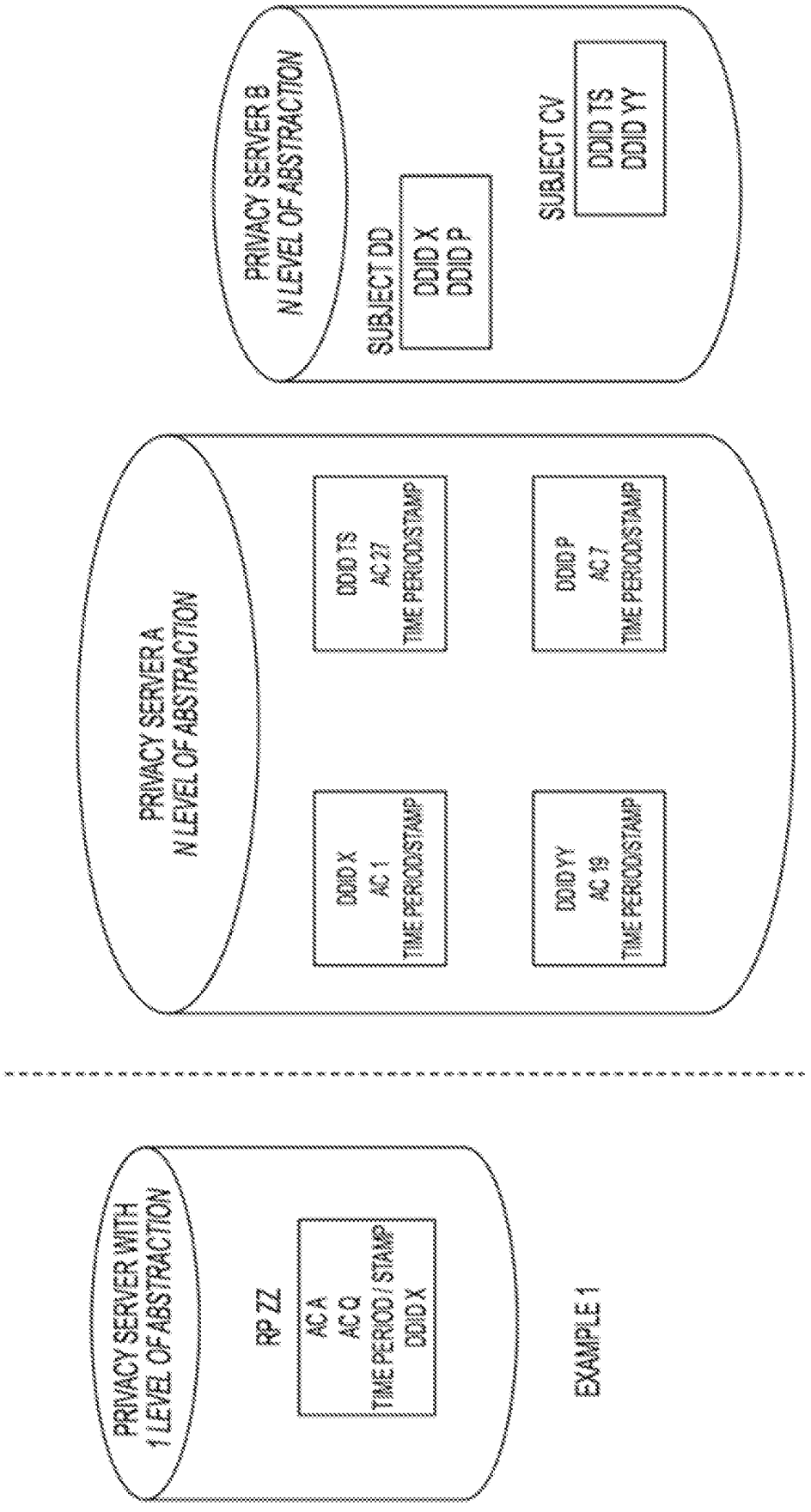

PRIVACY SERVER WITH
1 LEVEL OF ABSTRACTION
RP ZZ
AC A
AC Q
TIME PERIOD / STAMP
ODID X
EXAMPLE 1
PRIVACY SERVER A
N LEVEL OF ABSTRACTION
ODID X
AC 1
TIME PERIOD/STAMP
ODID TS
AC 27
TIME PERIOD/STAMP
ODID YY
AC 19
TIME PERIOD/STAMP
ODID P
AC 7
TIME PERIOD/STAMP
PRIVACY SERVER B
N LEVEL OF ABSTRACTION
SUBJECT DD
ODID X
ODID P
SUBJECT CV
ODID TS
ODID YY
EXAMPLE 2

FIG. 5

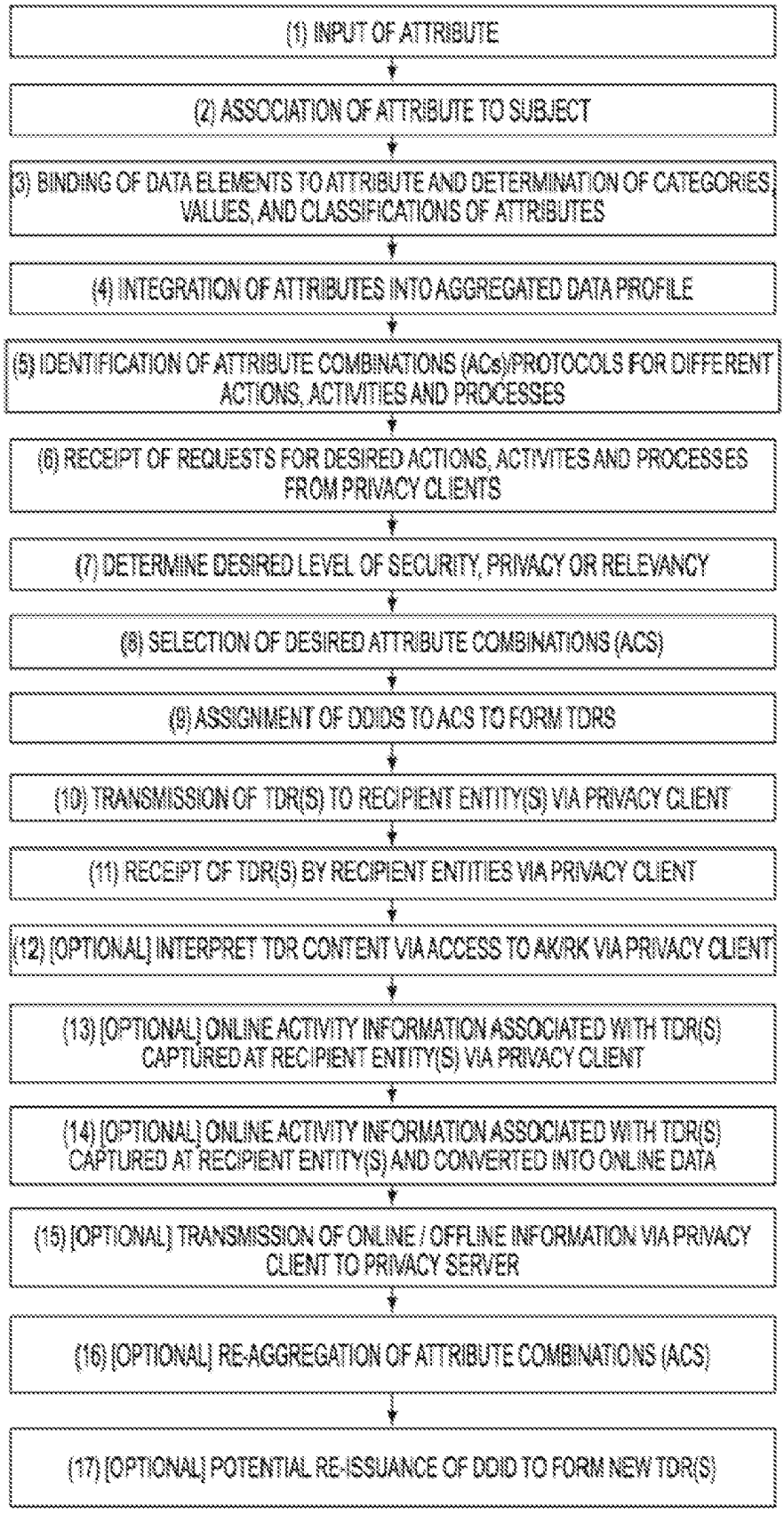

(1) INPUT OF ATTRIBUTE
(2) ASSOCIATION OF ATTRIBUTE TO SUBJECT
(3) BINDING OF DATA ELEMENTS TO ATTRIBUTE AND DETERMINATION OF CATEGORIES, VALUES, AND CLASSIFICATIONS OF ATTRIBUTES
(4) INTEGRATION OF ATTRIBUTES INTO AGGREGATED DATA PROFILE
(5) IDENTIFICATION OF ATTRIBUTE COMBINATIONS (ACs)/PROTOCOLS FOR DIFFERENT ACTIONS, ACTIVITIES AND PROCESSES
(6) RECEIPT OF REQUESTS FOR DESIRED ACTIONS, ACTIVITES AND PROCESSES FROM PRIVACY CLIENTS
(7) DETERMINE DESIRED LEVEL OF SECURITY, PRIVACY OR RELEVANCY
(8) SELECTION OF DESIRED ATTRIBUTE COMBINATIONS (ACS)
(9) ASSIGNMENT OF DDIDS TO ACS TO FORM TDRS
(10) TRANSMISSION OF TDR(S) TO RECIPIENT ENTITY(S) VIA PRIVACY CLIENT
(11) RECEIPT OF TDR(S) BY RECIPIENT ENTITIES VIA PRIVACY CLIENT
(12) [OPTIONAL] INTERPRET TDR CONTENT VIA ACCESS TO AK/RK VIA PRIVACY CLIENT
(13) [OPTIONAL] ONLINE ACTIVITY INFORMATION ASSOCIATED WITH TDR(S) CAPTURED AT RECIPIENT ENTITY(S) VIA PRIVACY CLIENT
(14) [OPTIONAL] ONLINE ACTIVITY INFORMATION ASSOCIATED WITH TDR(S) CAPTURED AT RECIPIENT ENTITY(S) AND CONVERTED INTO ONLINE DATA
(15) [OPTIONAL] TRANSMISSION OF ONLINE / OFFLINE INFORMATION VIA PRIVACY CLIENT TO PRIVACY SERVER
(16) [OPTIONAL] RE-AGGREGATION OF ATTRIBUTE COMBINATIONS (ACS)
(17) [OPTIONAL] POTENTIAL RE-ISSUANCE OF DDID TO FORM NEW TDR(S)

FIG. 6

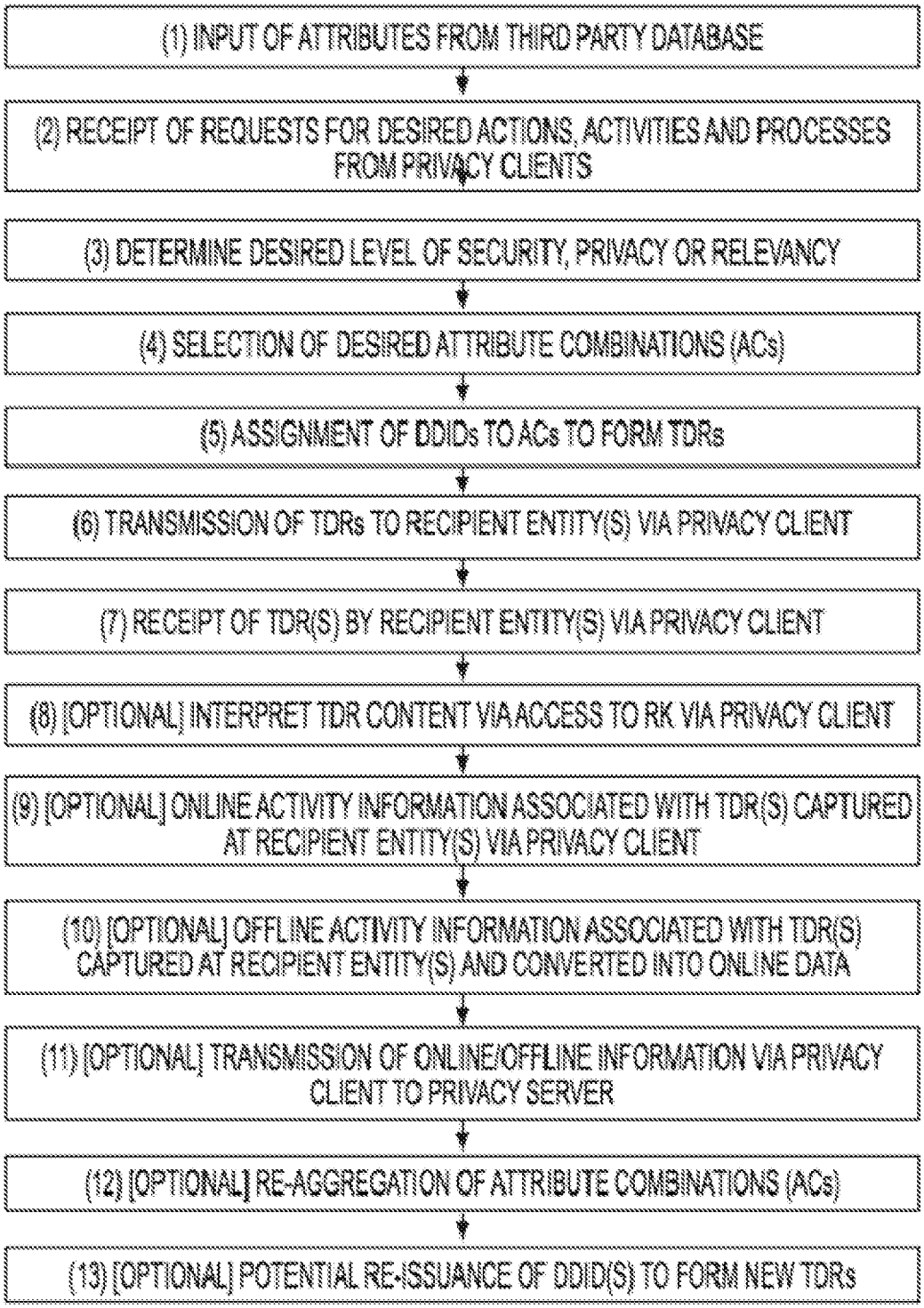

(1) INPUT OF ATTRIBUTES FROM THIRD PARTY DATABASE
(2) RECEIPT OF REQUESTS FOR DESIRED ACTIONS, ACTIVITIES AND PROCESSES FROM PRIVACY CLIENTS
(3) DETERMINE DESIRED LEVEL OF SECURITY, PRIVACY OR RELEVANCY
(4) SELECTION OF DESIRED ATTRIBUTE COMBINATIONS (ACs)
(5) ASSIGNMENT OF DDIDs TO ACs TO FORM TDRs
(6) TRANSMISSION OF TDRs TO RECIPIENT ENTITY(S) VIA PRIVACY CLIENT
(7) RECEIPT OF TDR(S) BY RECIPIENT ENTITY(S) VIA PRIVACY CLIENT
(8) [OPTIONAL] INTERPRET TDR CONTENT VIA ACCESS TO RK VIA PRIVACY CLIENT
(9) [OPTIONAL] ONLINE ACTIVITY INFORMATION ASSOCIATED WITH TDR(S) CAPTURED AT RECIPIENT ENTITY(S) VIA PRIVACY CLIENT
(10) [OPTIONAL] OFFLINE ACTIVITY INFORMATION ASSOCIATED WITH TDR(S) CAPTURED AT RECIPIENT ENTITY(S) AND CONVERTED INTO ONLINE DATA
(11) [OPTIONAL] TRANSMISSION OF ONLINE/OFFLINE INFORMATION VIA PRIVACY CLIENT TO PRIVACY SERVER
(12) [OPTIONAL] RE-AGGREGATION OF ATTRIBUTE COMBINATIONS (ACs)
(13) [OPTIONAL] POTENTIAL RE-ISSUANCE OF DDID(S) TO FORM NEW TDRs

FIG. 6A

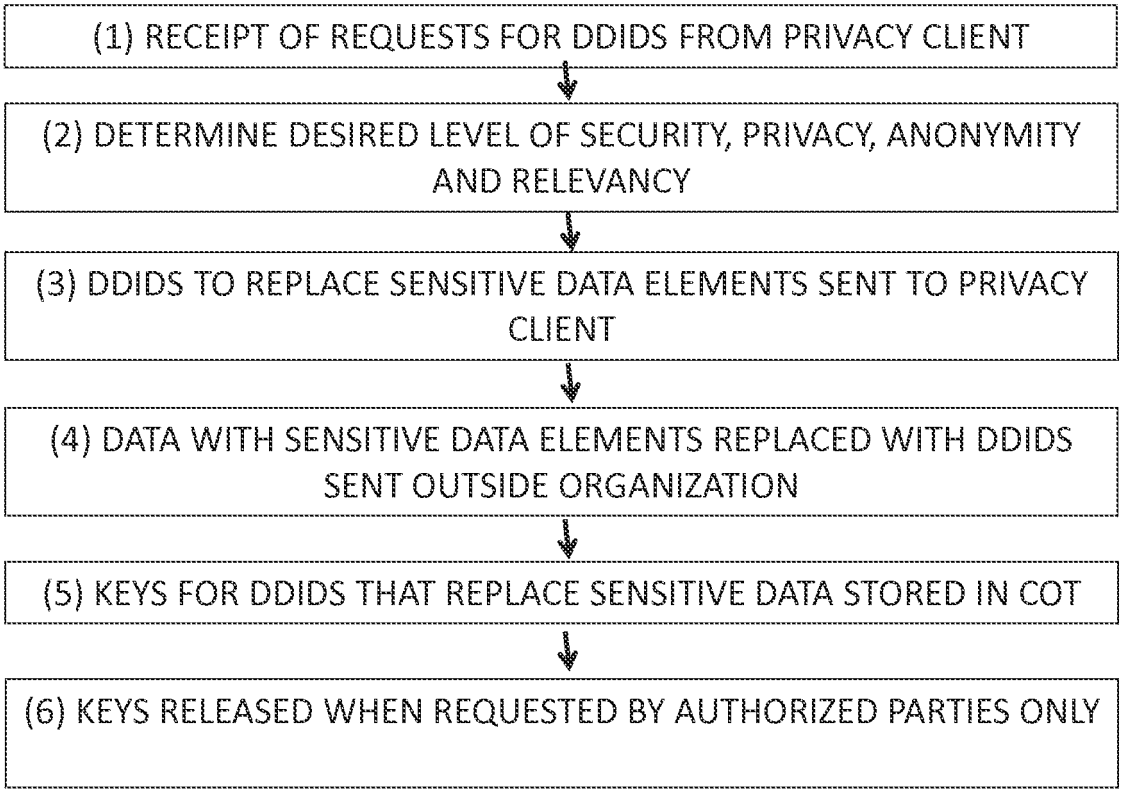

(1) RECEIPT OF REQUESTS FOR DDIDS FROM PRIVACY CLIENT
(2) DETERMINE DESIRED LEVEL OF SECURITY, PRIVACY, ANONYMITY AND RELEVANCY
(3) DDIDS TO REPLACE SENSITIVE DATA ELEMENTS SENT TO PRIVACY CLIENT
(4) DATA WITH SENSITIVE DATA ELEMENTS REPLACED WITH DDIDS SENT OUTSIDE ORGANIZATION
(5) KEYS FOR DDIDS THAT REPLACE SENSITIVE DATA STORED IN COT
(6) KEYS RELEASED WHEN REQUESTED BY AUTHORIZED PARTIES ONLY

FIG. 6B

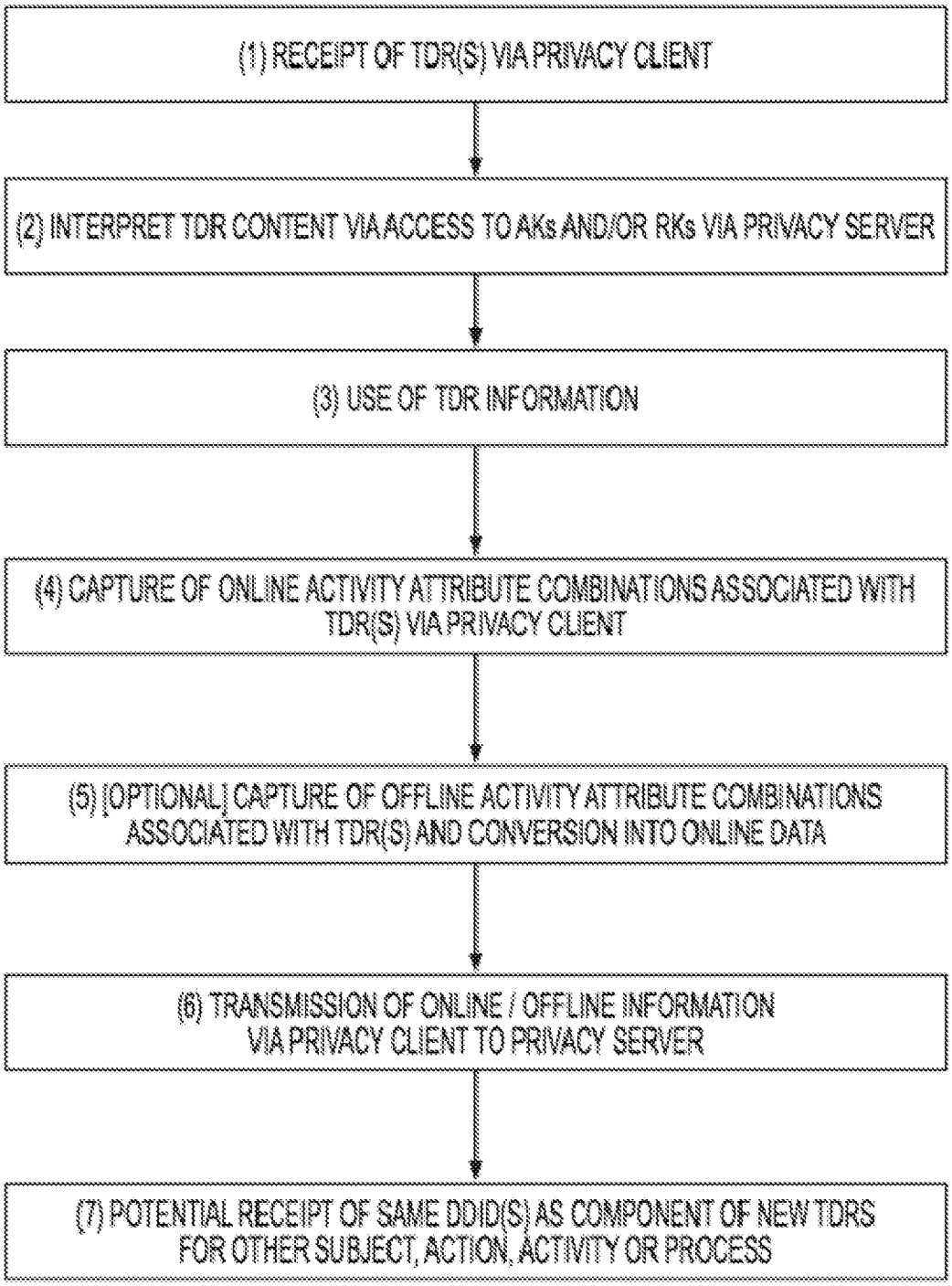

(1) RECEIPT OF TDR(S) VIA PRIVACY CLIENT
(2) INTERPRET TDR CONTENT VIA ACCESS TO AKs AND/OR RKs VIA PRIVACY SERVER
(3) USE OF TDR INFORMATION
(4) CAPTURE OF ONLINE ACTIVITY ATTRIBUTE COMBINATIONS ASSOCIATED WITH TDR(S) VIA PRIVACY CLIENT
(5) [OPTIONAL] CAPTURE OF OFFLINE ACTIVITY ATTRIBUTE COMBINATIONS ASSOCIATED WITH TDR(S) AND CONVERSION INTO ONLINE DATA
(6) TRANSMISSION OF ONLINE / OFFLINE INFORMATION VIA PRIVACY CLIENT TO PRIVACY SERVER
(7) POTENTIAL RECEIPT OF SAME DDID(S) AS COMPONENT OF NEW TDRS FOR OTHER SUBJECT, ACTION, ACTIVITY OR PROCESS

FIG. 7

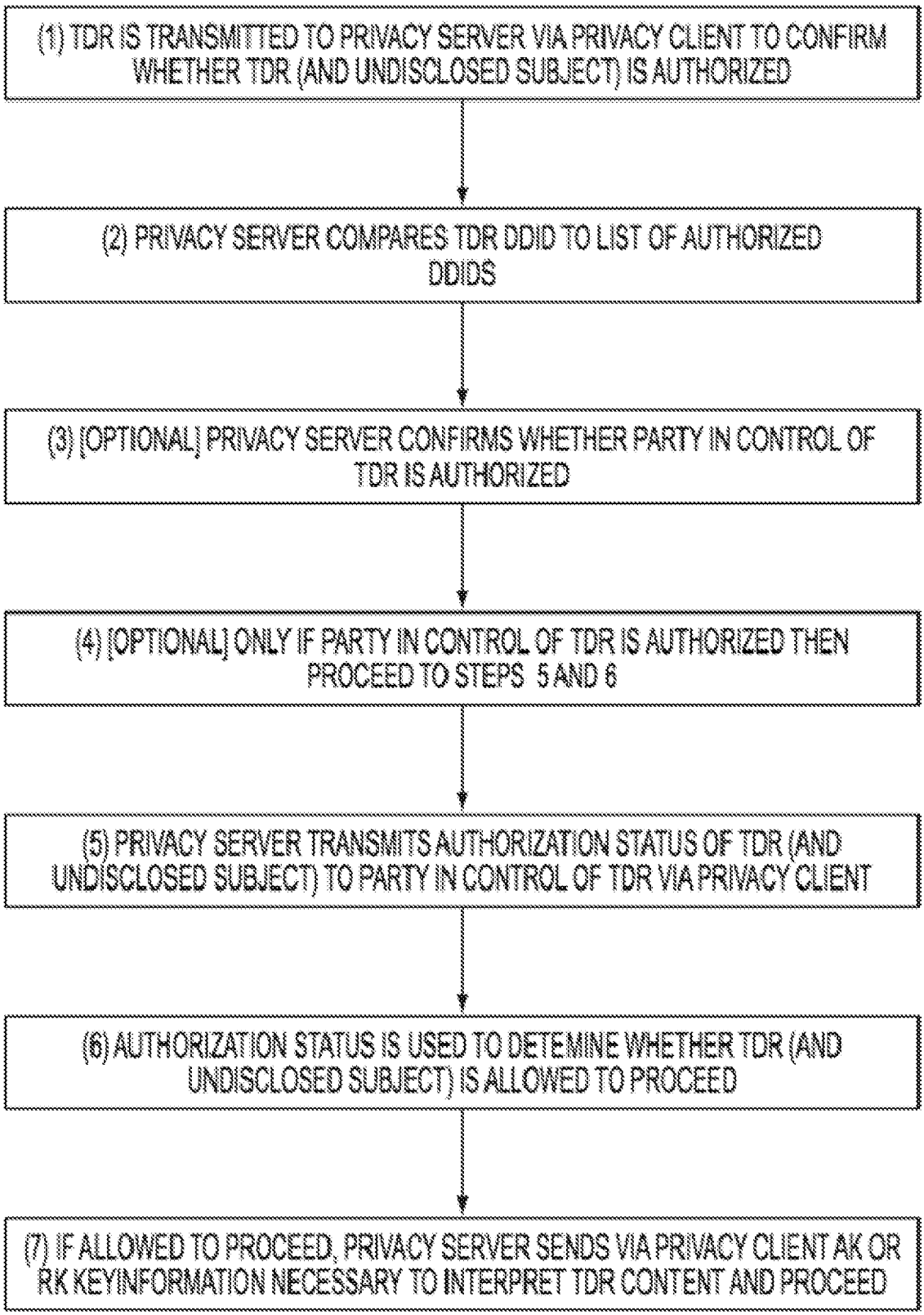

(1) TDR IS TRANSMITTED TO PRIVACY SERVER VIA PRIVACY CLIENT TO CONFIRM WHETHER TDR (AND UNDISCLOSED SUBJECT) IS AUTHORIZED
(2) PRIVACY SERVER COMPARES TDR DDID TO LIST OF AUTHORIZED DDIDS
(3) [OPTIONAL] PRIVACY SERVER CONFIRMS WHETHER PARTY IN CONTROL OF TDR IS AUTHORIZED
(4) [OPTIONAL] ONLY IF PARTY IN CONTROL OF TDR IS AUTHORIZED THEN PROCEED TO STEPS 5 AND 6
(5) PRIVACY SERVER TRANSMITS AUTHORIZATION STATUS OF TDR (AND UNDISCLOSED SUBJECT) TO PARTY IN CONTROL OF TDR VIA PRIVACY CLIENT
(6) AUTHORIZATION STATUS IS USED TO DETEMINE WHETHER TDR (AND UNDISCLOSED SUBJECT) IS ALLOWED TO PROCEED
(7) IF ALLOWED TO PROCEED, PRIVACY SERVER SENDS VIA PRIVACY CLIENT AK OR RK KEYINFORMATION NECESSARY TO INTERPRET TDR CONTENT AND PROCEED

FIG. 8

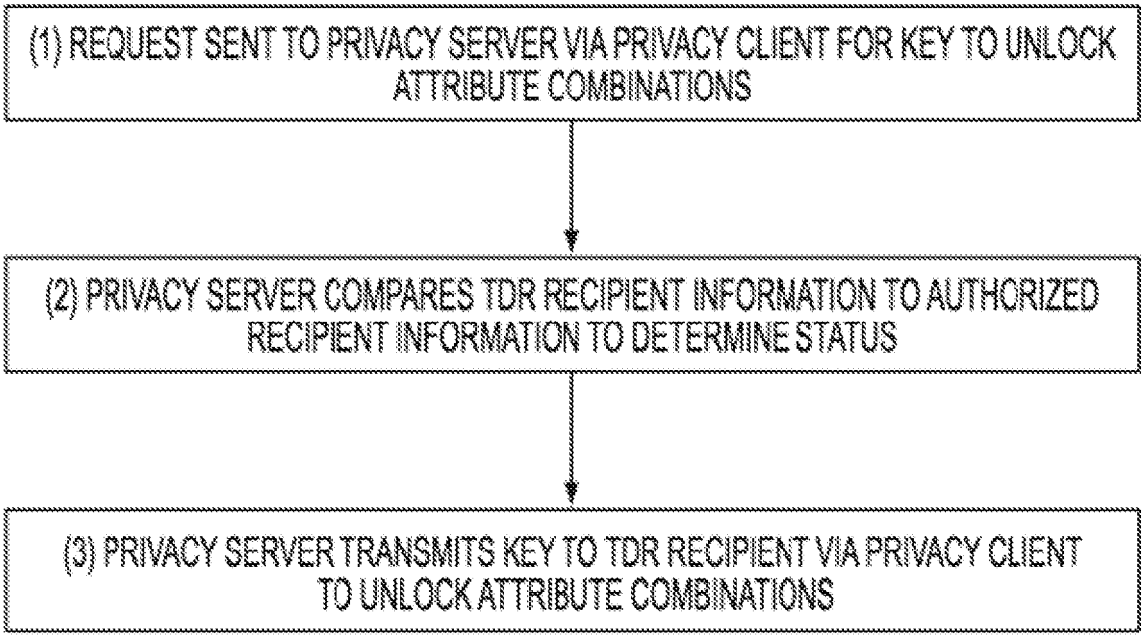

(1) REQUEST SENT TO PRIVACY SERVER VIA PRIVACY CLIENT FOR KEY TO UNLOCK ATTRIBUTE COMBINATIONS
(2) PRIVACY SERVER COMPARES TDR RECIPIENT INFORMATION TO AUTHORIZED RECIPIENT INFORMATION TO DETERMINE STATUS
(3) PRIVACY SERVER TRANSMITS KEY TO TDR RECIPIENT VIA PRIVACY CLIENT TO UNLOCK ATTRIBUTE COMBINATIONS

FIG. 9

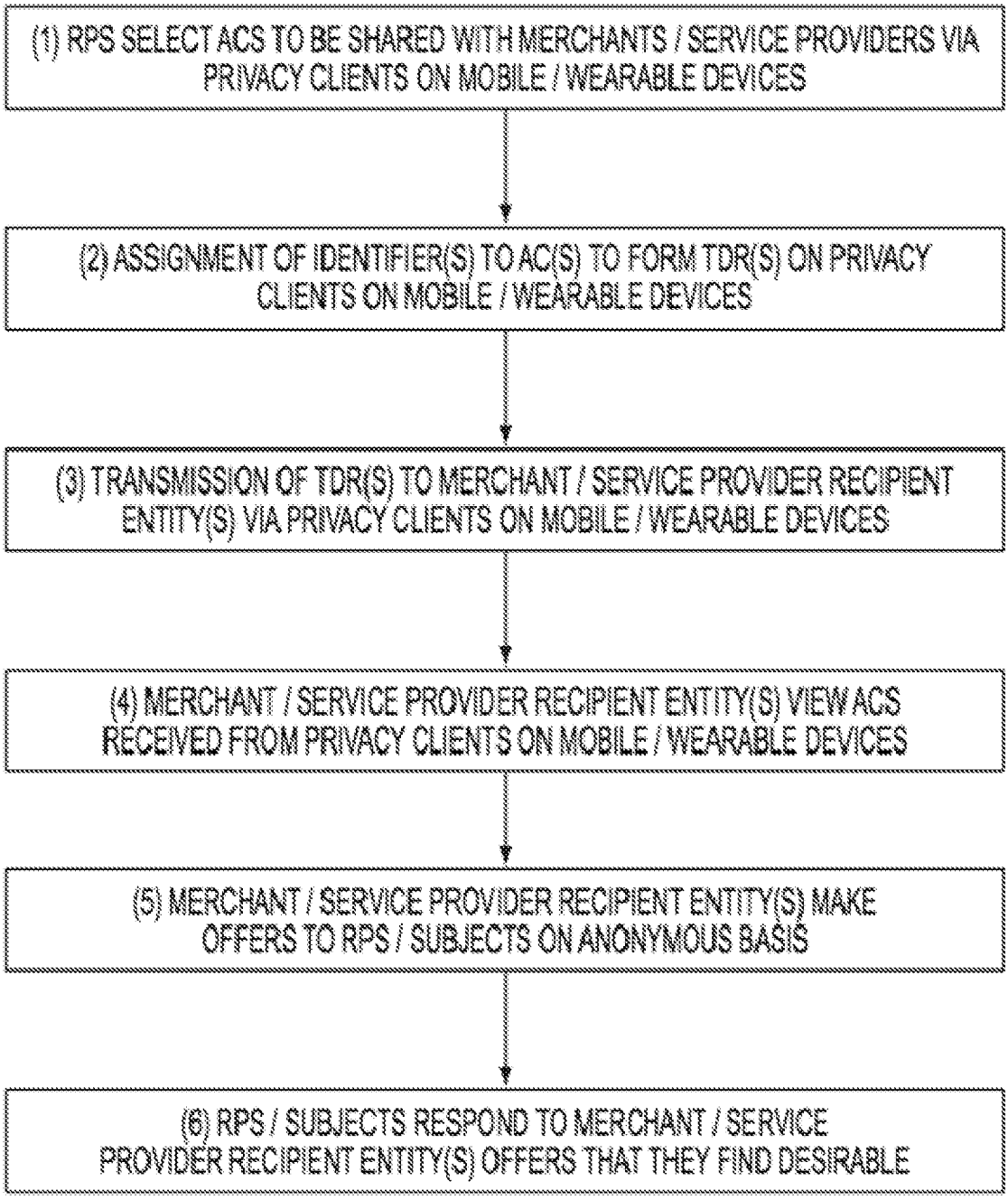

(1) RPS SELECT ACS TO BE SHARED WITH MERCHANTS / SERVICE PROVIDERS VIA PRIVACY CLIENTS ON MOBILE / WEARABLE DEVICES
(2) ASSIGNMENT OF IDENTIFIER(S) TO AC(S) TO FORM TDR(S) ON PRIVACY CLIENTS ON MOBILE / WEARABLE DEVICES
(3) TRANSMISSION OF TDR(S) TO MERCHANT / SERVICE PROVIDER RECIPIENT ENTITY(S) VIA PRIVACY CLIENTS ON MOBILE / WEARABLE DEVICES
(4) MERCHANT / SERVICE PROVIDER RECIPIENT ENTITY(S) VIEW ACS RECEIVED FROM PRIVACY CLIENTS ON MOBILE / WEARABLE DEVICES
(5) MERCHANT / SERVICE PROVIDER RECIPIENT ENTITY(S) MAKE OFFERS TO RPS / SUBJECTS ON ANONYMOUS BASIS
(6) RPS / SUBJECTS RESPOND TO MERCHANT / SERVICE PROVIDER RECIPIENT ENTITY(S) OFFERS THAT THEY FIND DESIRABLE

FIG. 10

FIG. 11

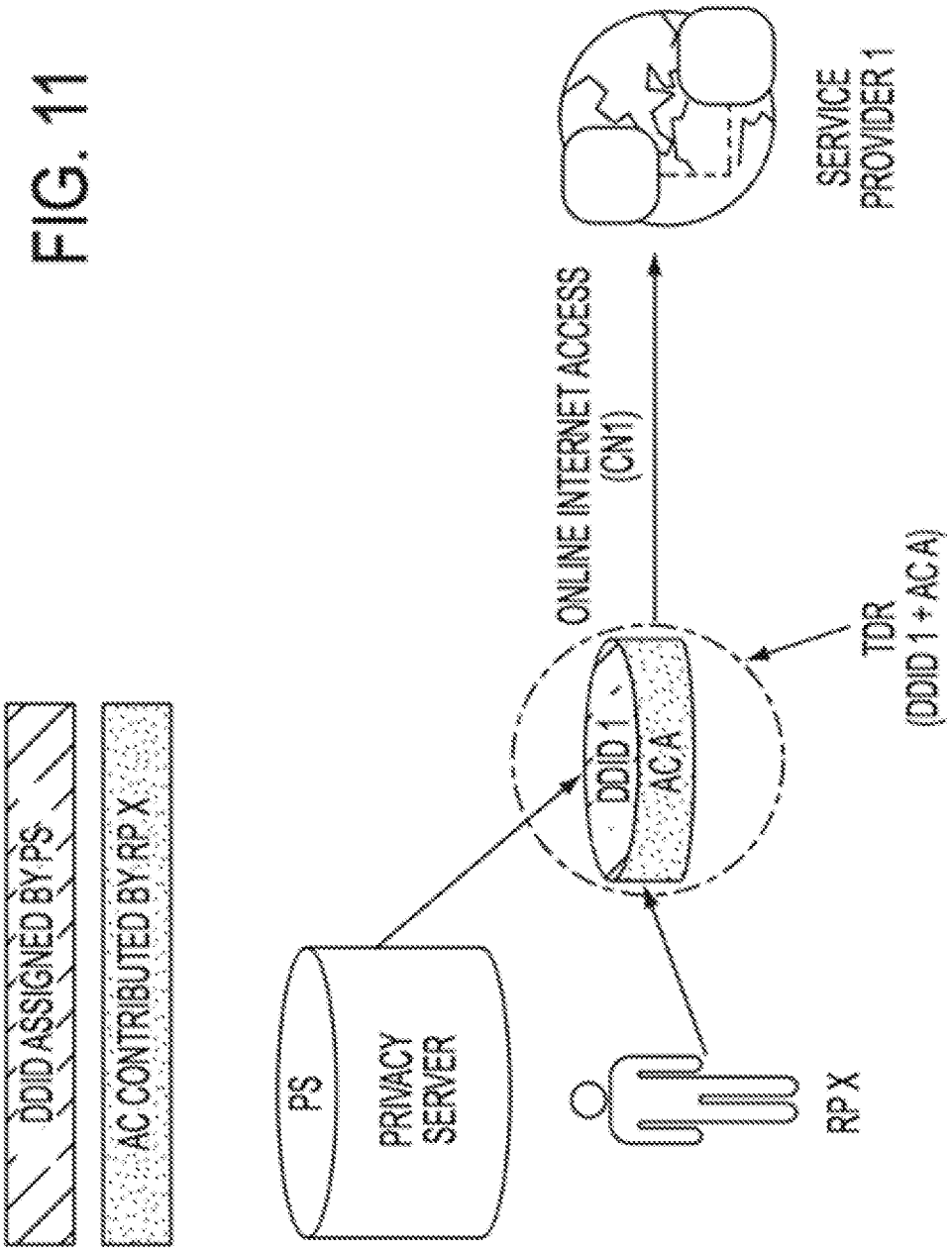

ODID ASSIGNED BY PS
AC CONTRIBUTED BY RP X
PS
PRIVACY SERVER
RP X
ODID 1 + ACA
TDR (ODID 1 + ACA)
ONLINE INTERNET ACCESS (CN1)
SERVICE PROVIDER 1

FIG. 12

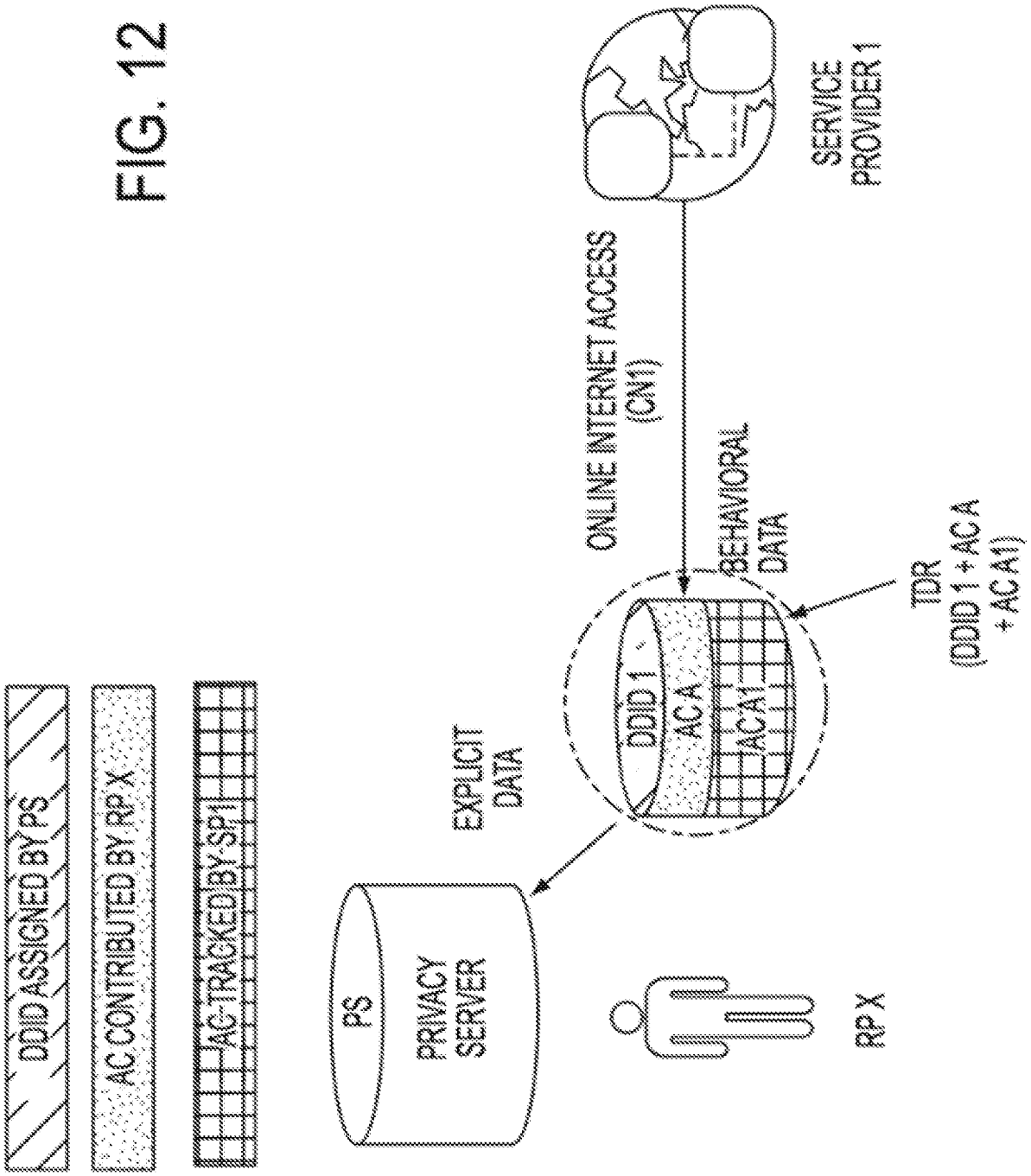

DDID ASSIGNED BY PS
AC CONTRIBUTED BY RP X
AC TRACKED BY SP1
PS
PRIVACY SERVER
EXPLICIT DATA
DDID 1
AC A
ACA1
BEHAVIORAL DATA
ONLINE INTERNET ACCESS (CN1)
TDR (DDID 1 + AC A + AC A1)
SERVICE PROVIDER 1
RP X

FIG. 13

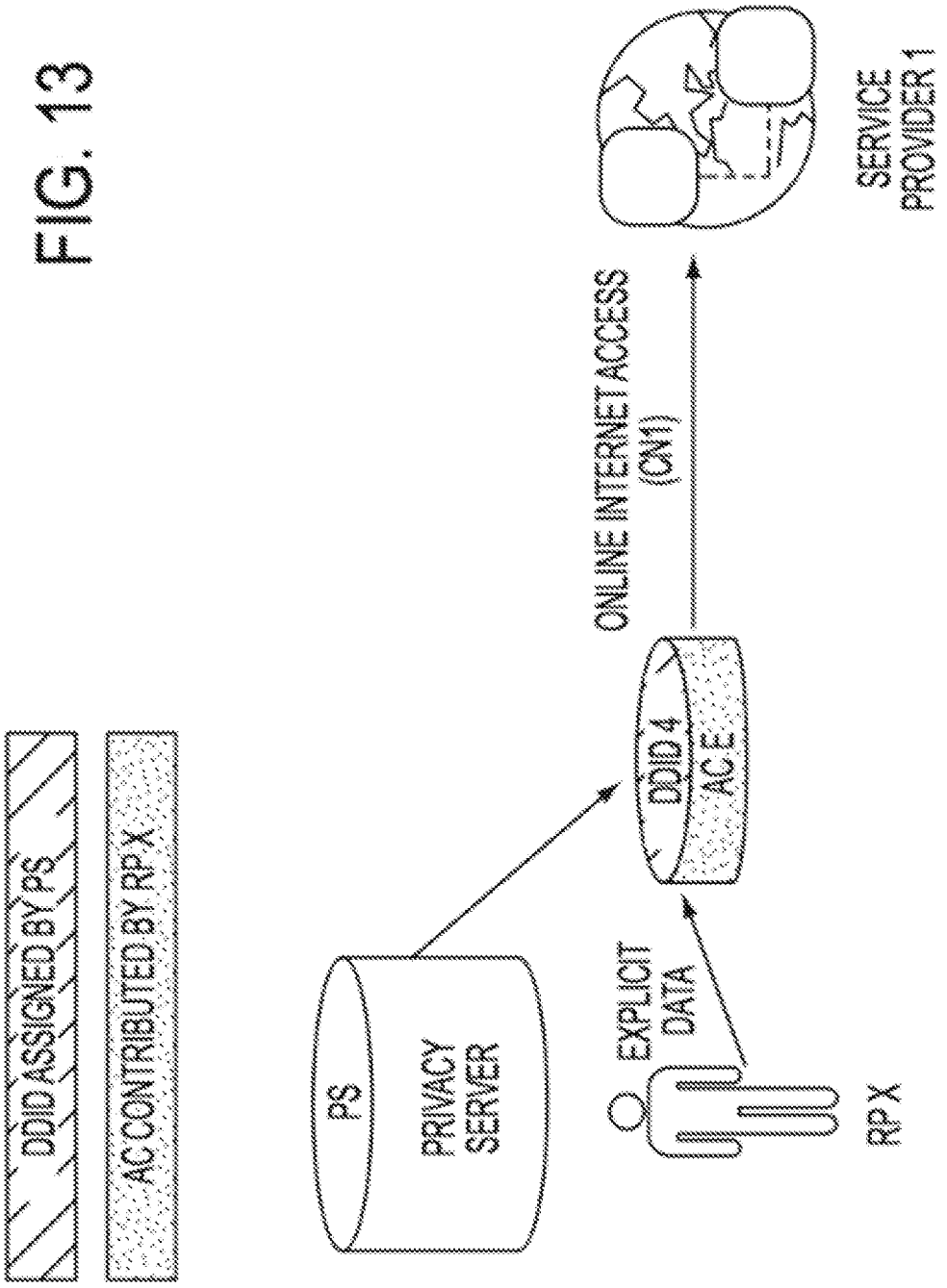

DDID ASSIGNED BY PS
AC CONTRIBUTED BY RP X
PS
PRIVACY SERVER
EXPLICIT DATA
DDID 4
ACE
RP X
ONLINE INTERNET ACCESS (CN1)
SERVICE PROVIDER 1

FIG. 14

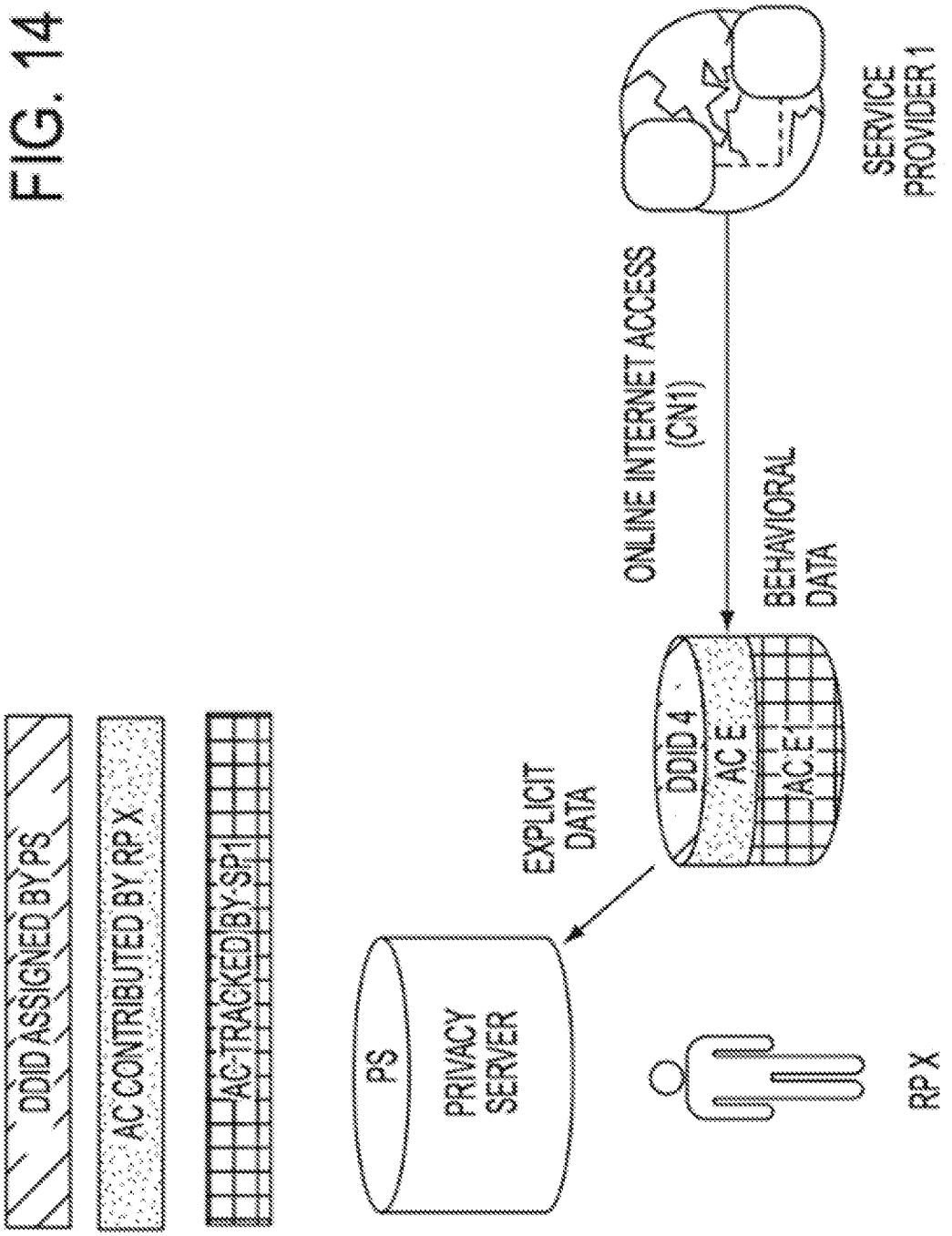

DDID ASSIGNED BY PS
AC CONTRIBUTED BY RP X
AC TRACKED BY SP1
PS
PRIVACY SERVER
EXPLICIT DATA
DDID 4
AC E
AC E1
ONLINE INTERNET ACCESS (CN1)
BEHAVIORAL DATA
SERVICE PROVIDER 1
RP X

FIG. 15

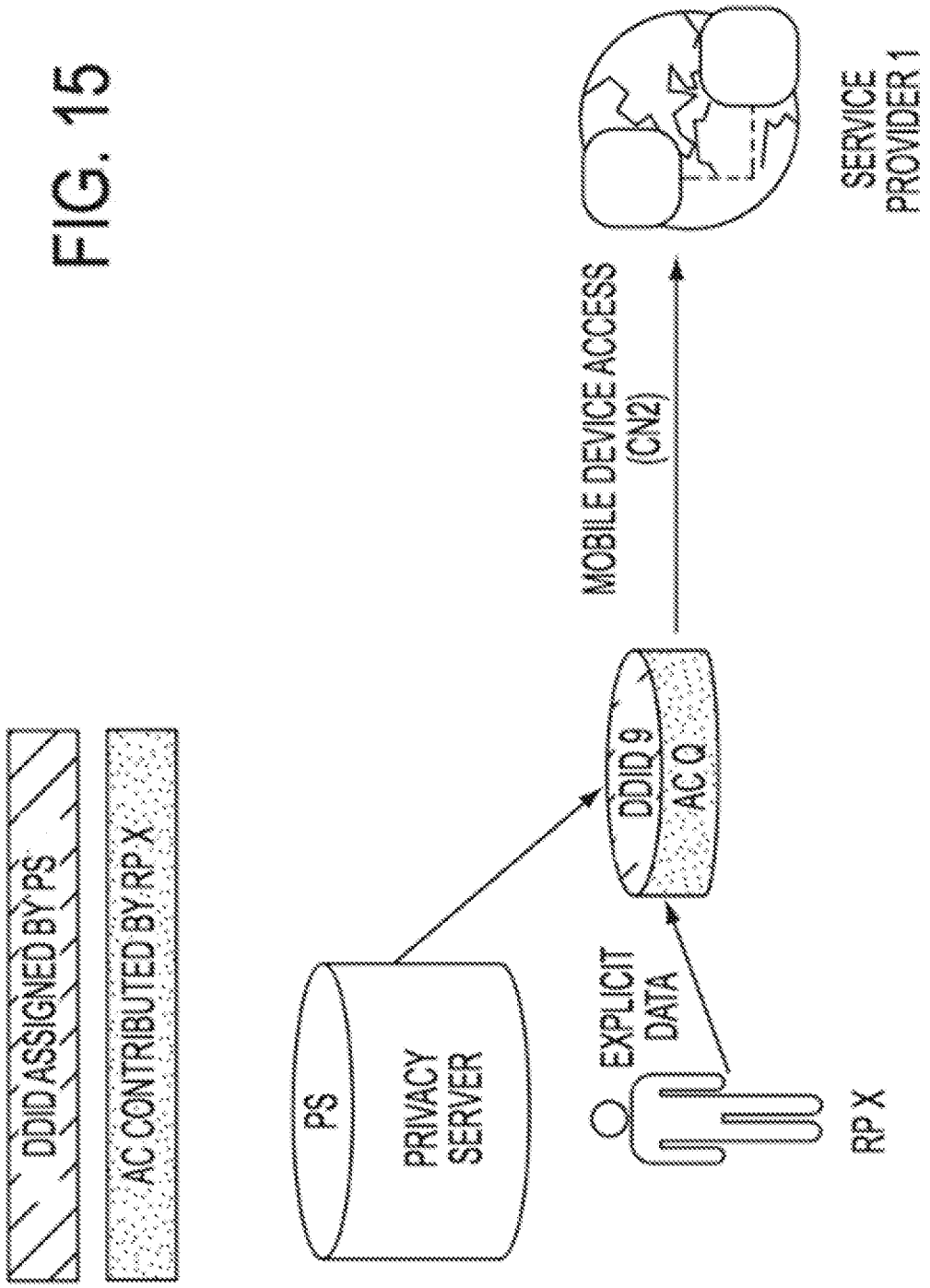

DDID ASSIGNED BY PS
AC CONTRIBUTED BY RP X
PS
PRIVACY SERVER
DDID 9
AC Q
EXPLICIT DATA
RP X
MOBILE DEVICE ACCESS (CN2)
SERVICE PROVIDER 1

FIG. 16

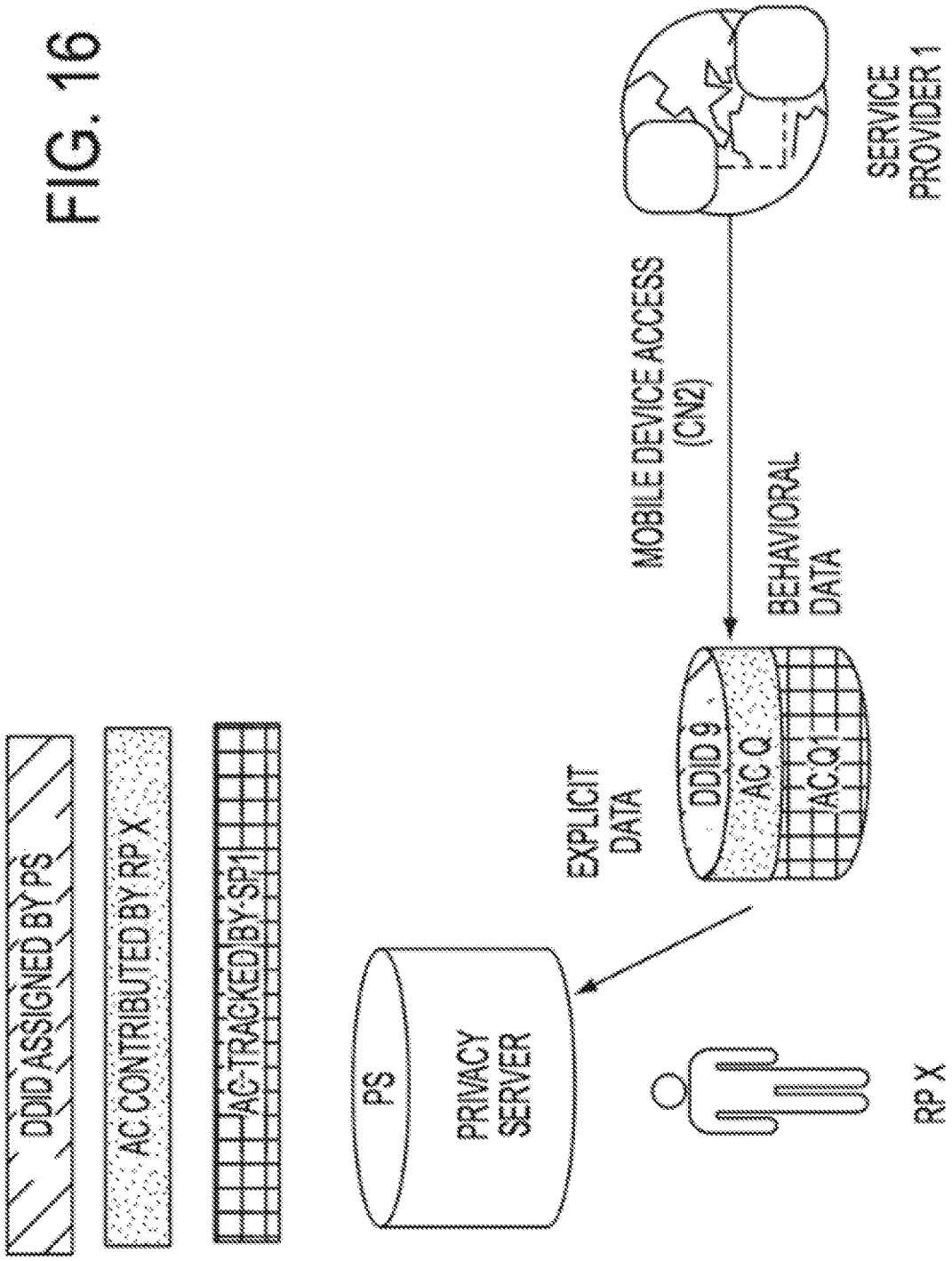

DDID ASSIGNED BY PS
AC CONTRIBUTED BY RP X
AC TRACKED BY SP1
PS
PRIVACY SERVER
EXPLICIT DATA
DDID 9
AC Q
AC Q1
BEHAVIORAL DATA
MOBILE DEVICE ACCESS (CN2)
SERVICE PROVIDER 1
RP X

FIG. 17

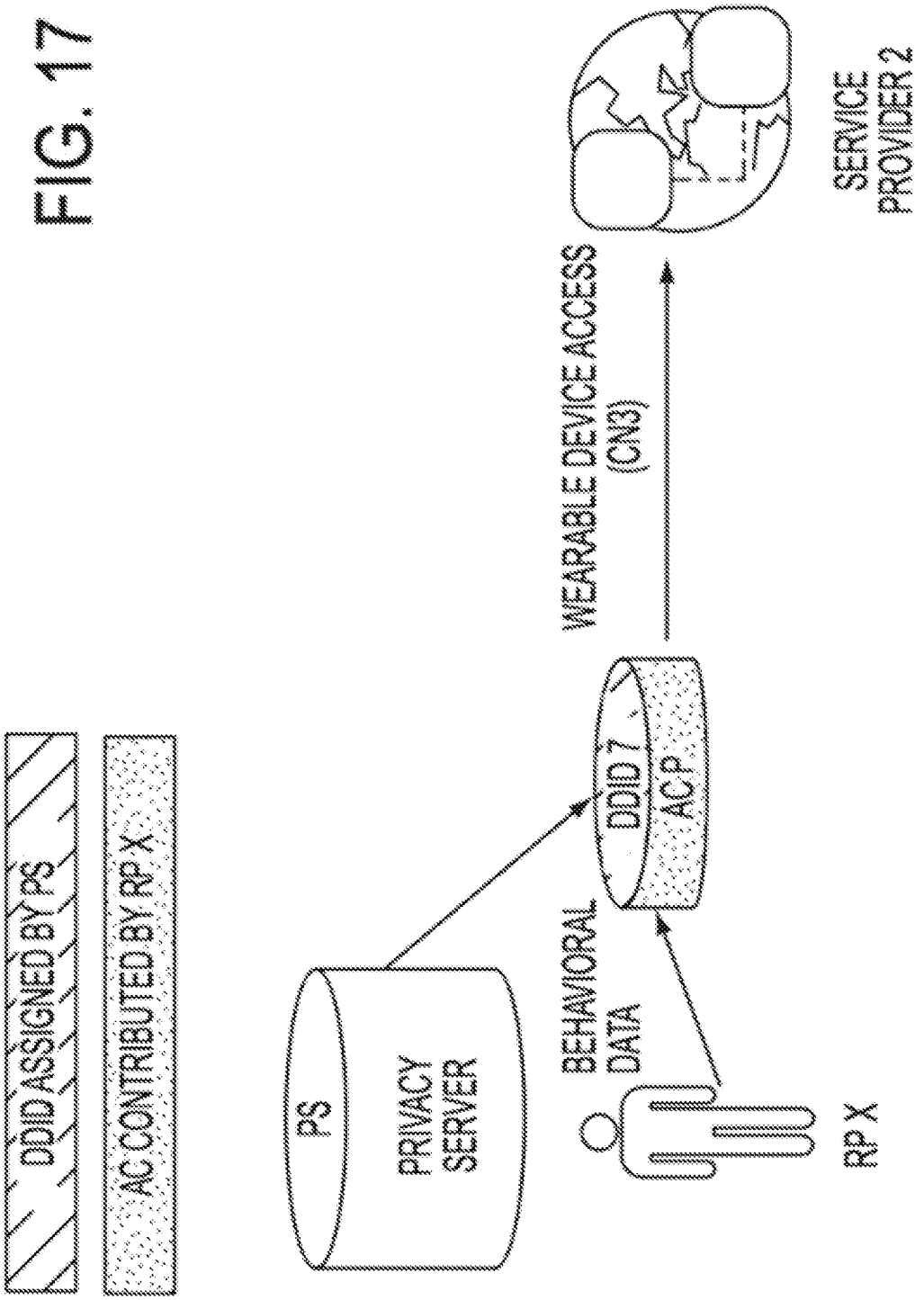

DDID ASSIGNED BY PS
AC CONTRIBUTED BY RP X
PS
PRIVACY SERVER
BEHAVIORAL DATA
DDID 7
ACP
RP X
WEARABLE DEVICE ACCESS (CN3)
SERVICE PROVIDER 2

FIG. 18

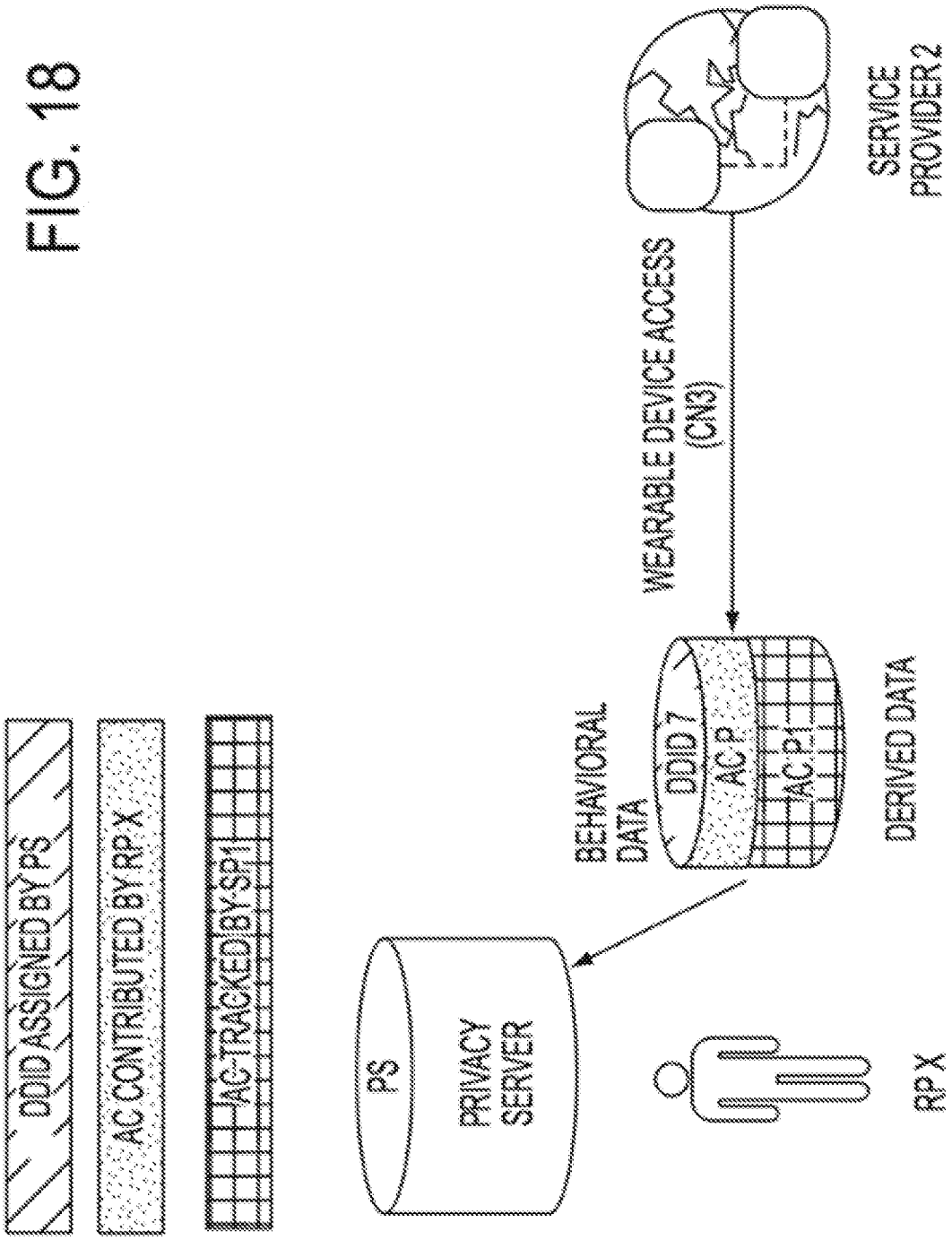

ODID ASSIGNED BY PS
AC CONTRIBUTED BY RP X
AC TRACKED BY SP1
PS
PRIVACY SERVER
RP X
BEHAVIORAL DATA
ODID 7
AC P
AC P1
DERIVED DATA
WEARABLE DEVICE ACCESS (CN3)
SERVICE PROVIDER 2

FIG. 19

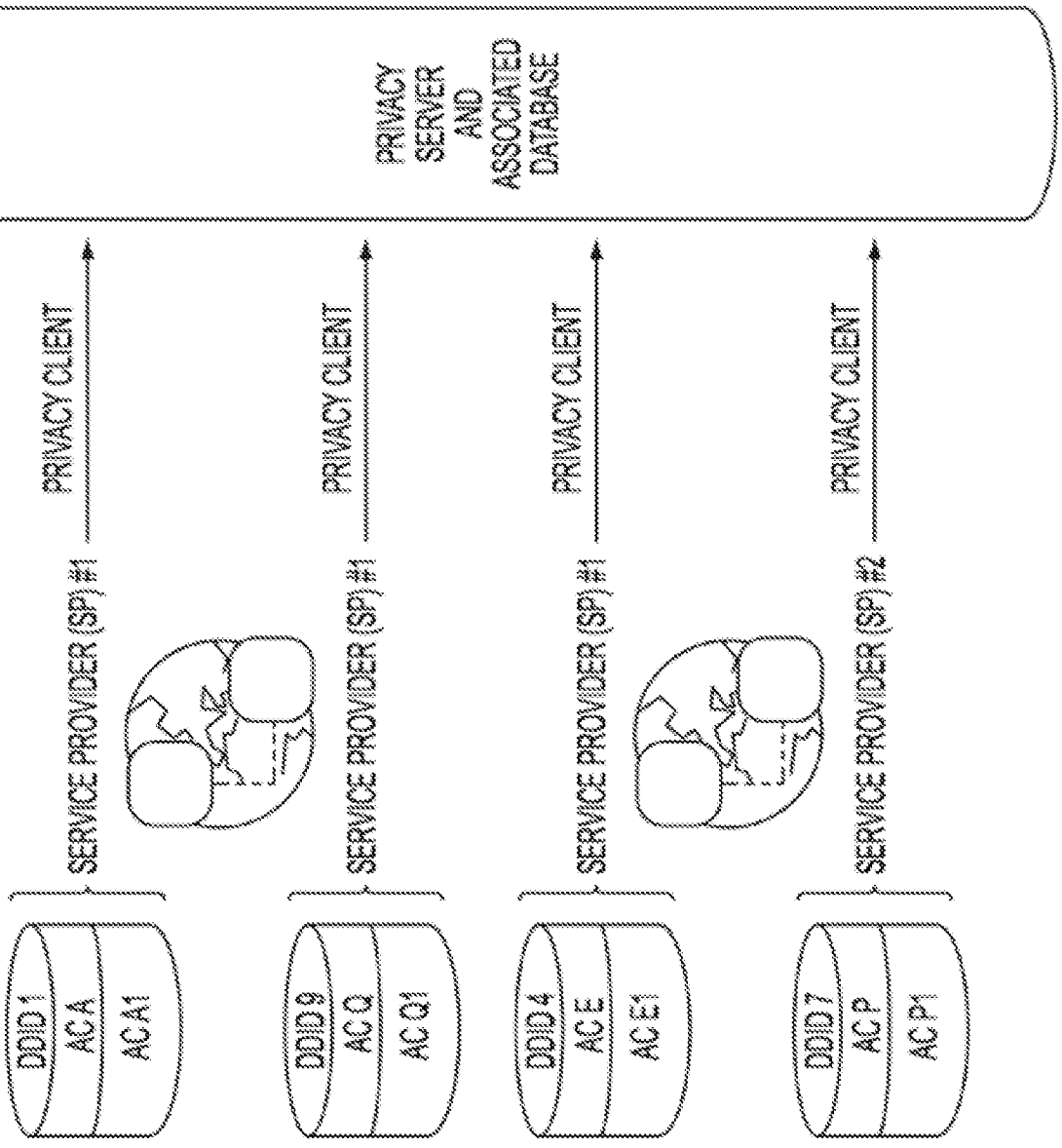
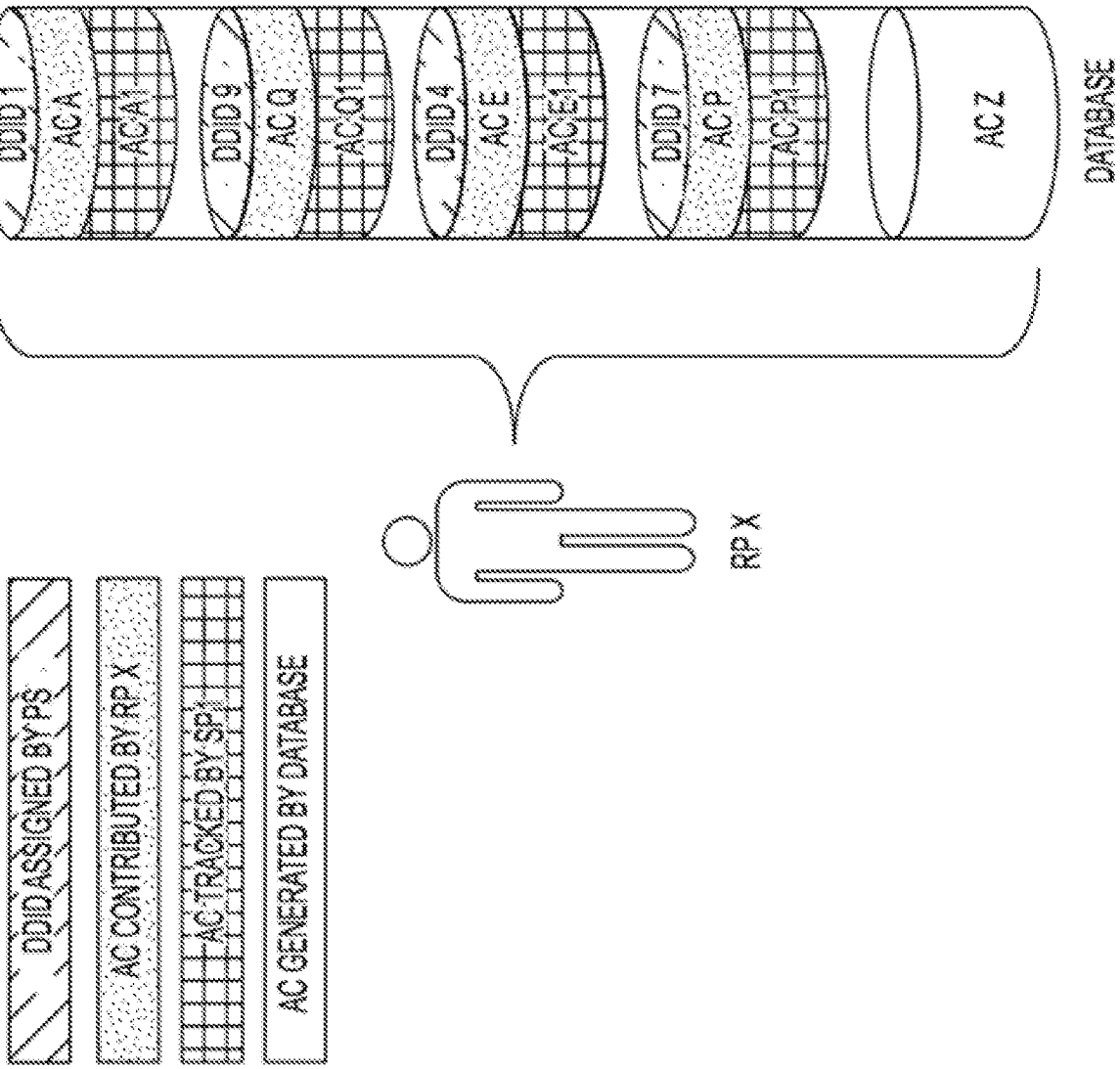

PRIVACY SERVER AND ASSOCIATED DATABASE
PRIVACY CLIENT
PRIVACY CLIENT
PRIVACY CLIENT
PRIVACY CLIENT
SERVICE PROVIDER (SP) #1
SERVICE PROVIDER (SP) #1
SERVICE PROVIDER (SP) #1
SERVICE PROVIDER (SP) #2
DDID 1
AC A
AC A1
DDID 9
AC Q
AC Q1
DDID 4
AC E
AC E1
DDID 7
AC P
AC P1

FIG. 20


DDID 1
AC A
ACA1
DDID 9
AC Q
ACQ1
DDID 4
AC E
ACE1
DDID 7
AC P
ACP1
AC Z
DATABASE
RP X
DDID ASSIGNED BY PS
AC CONTRIBUTED BY RP X
AC TRACKED BY SP1
AC GENERATED BY DATABASE

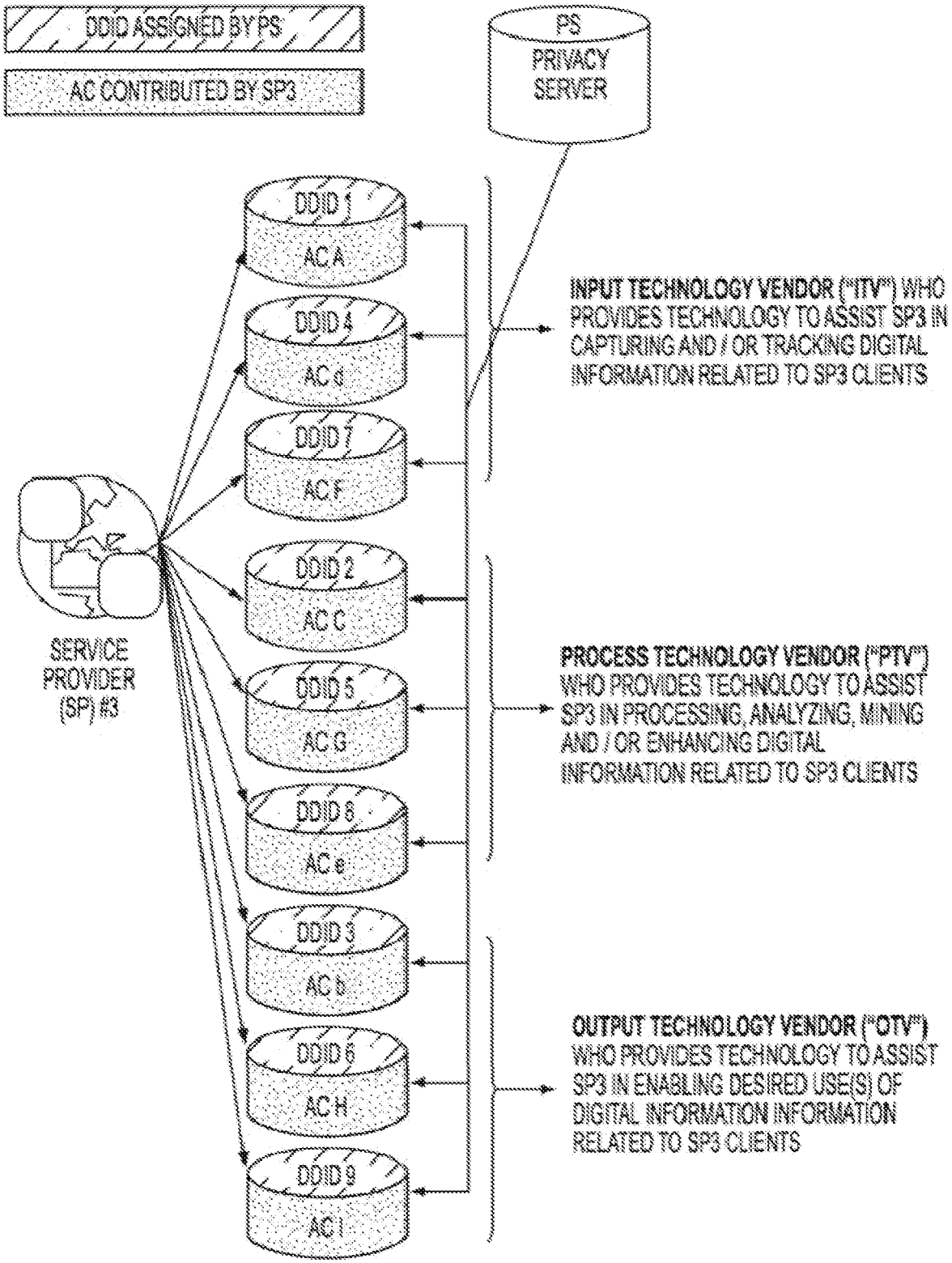

DDID ASSIGNED BY PS
AC CONTRIBUTED BY SP3
PS
PRIVACY
SERVER
DDID 1
AC A
DDID 4
AC d
DDID 7
AC F
DDID 2
AC C
DDID 5
AC G
DDID 8
AC e
DDID 3
AC b
DDID 6
AC H
DDID 9
AC I
SERVICE
PROVIDER
(SP) #3
INPUT TECHNOLOGY VENDOR ("ITV") WHO PROVIDES TECHNOLOGY TO ASSIST SP3 IN CAPTURING AND / OR TRACKING DIGITAL INFORMATION RELATED TO SP3 CLIENTS
PROCESS TECHNOLOGY VENDOR ("PTV") WHO PROVIDES TECHNOLOGY TO ASSIST SP3 IN PROCESSING, ANALYZING, MINING AND / OR ENHANCING DIGITAL INFORMATION RELATED TO SP3 CLIENTS
OUTPUT TECHNOLOGY VENDOR ("OTV") WHO PROVIDES TECHNOLOGY TO ASSIST SP3 IN ENABLING DESIRED USE(S) OF DIGITAL INFORMATION INFORMATION RELATED TO SP3 CLIENTS

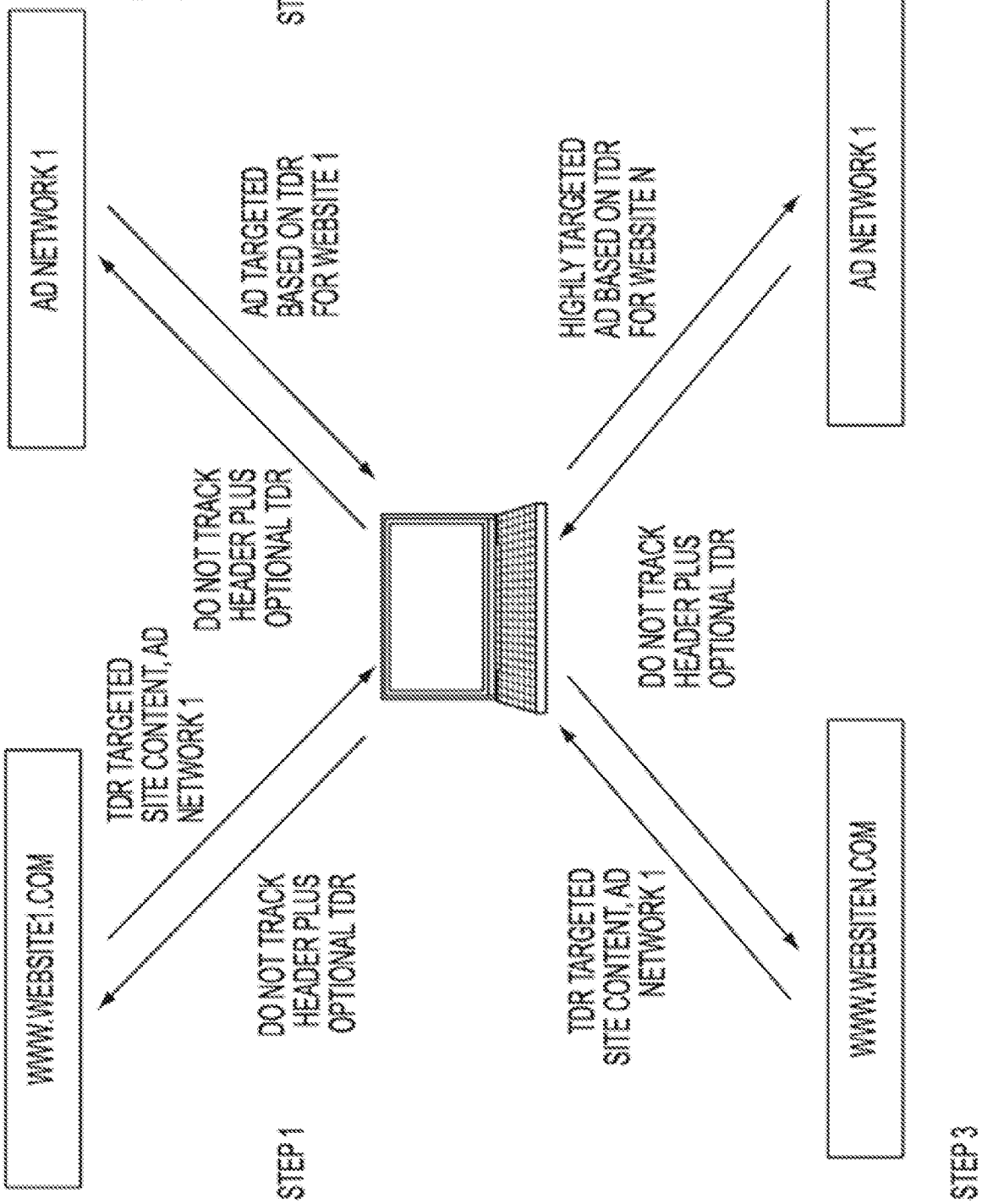
FIG. 21

FIG. 22

PRIVACY SERVER AND ASSOCIATED DATABASE

ATTRIBUTE COMBINATIONS	DOIDS
INPUT TECHNOLOGY PROVIDER	
A	1
d	4
F	7
PROCESS TECHNOLOGY PROVIDER	
C	2
G	5
e	8
OUTPUT TECHNOLOGY PROVIDER	
b	3
H	6
I	9

FIG. 23


AD NETWORK 1
AD TARGETED BASED ON TDR FOR WEBSITE 1
STEP 2
HIGHLY TARGETED AD BASED ON TDR FOR WEBSITE N
AD NETWORK 1
DO NOT TRACK HEADER PLUS OPTIONAL TDR
TDR TARGETED SITE CONTENT, AD NETWORK 1
DO NOT TRACK HEADER PLUS OPTIONAL TDR
WWW.WEBSITE1.COM
STEP 1
DO NOT TRACK HEADER PLUS OPTIONAL TDR
TDR TARGETED SITE CONTENT, AD NETWORK 1
WWW.WEBSITEN.COM
STEP 3

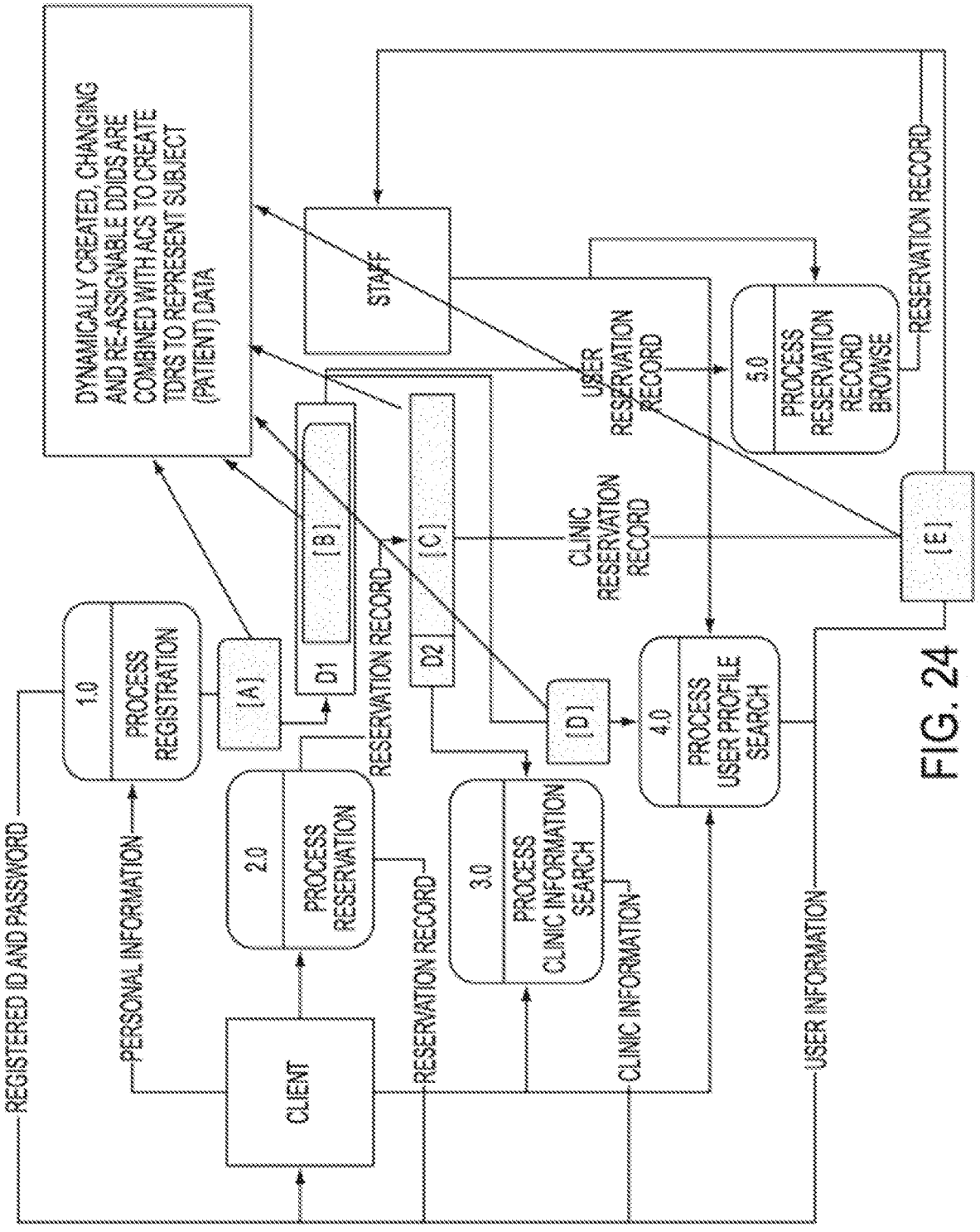

DYNAMICALLY CREATED, CHANGING AND RE-ASSIGNABLE DDIDS ARE COMBINED WITH ACS TO CREATE TDRS TO REPRESENT SUBJECT (PATIENT) DATA
STAFF
USER RESERVATION RECORD
5.0 PROCESS RESERVATION RECORD BROWSE
RESERVATION RECORD
CLINIC RESERVATION RECORD
[E]
[B]
D1
[C]
D2
[A]
1.0 PROCESS REGISTRATION
2.0 PROCESS RESERVATION
[D]
4.0 PROCESS USER PROFILE SEARCH
3.0 PROCESS CLINIC INFORMATION SEARCH
RESERVATION RECORD
CLIENT
REGISTERED ID AND PASSWORD
PERSONAL INFORMATION
RESERVATION RECORD
CLINIC INFORMATION
USER INFORMATION

FIG. 24

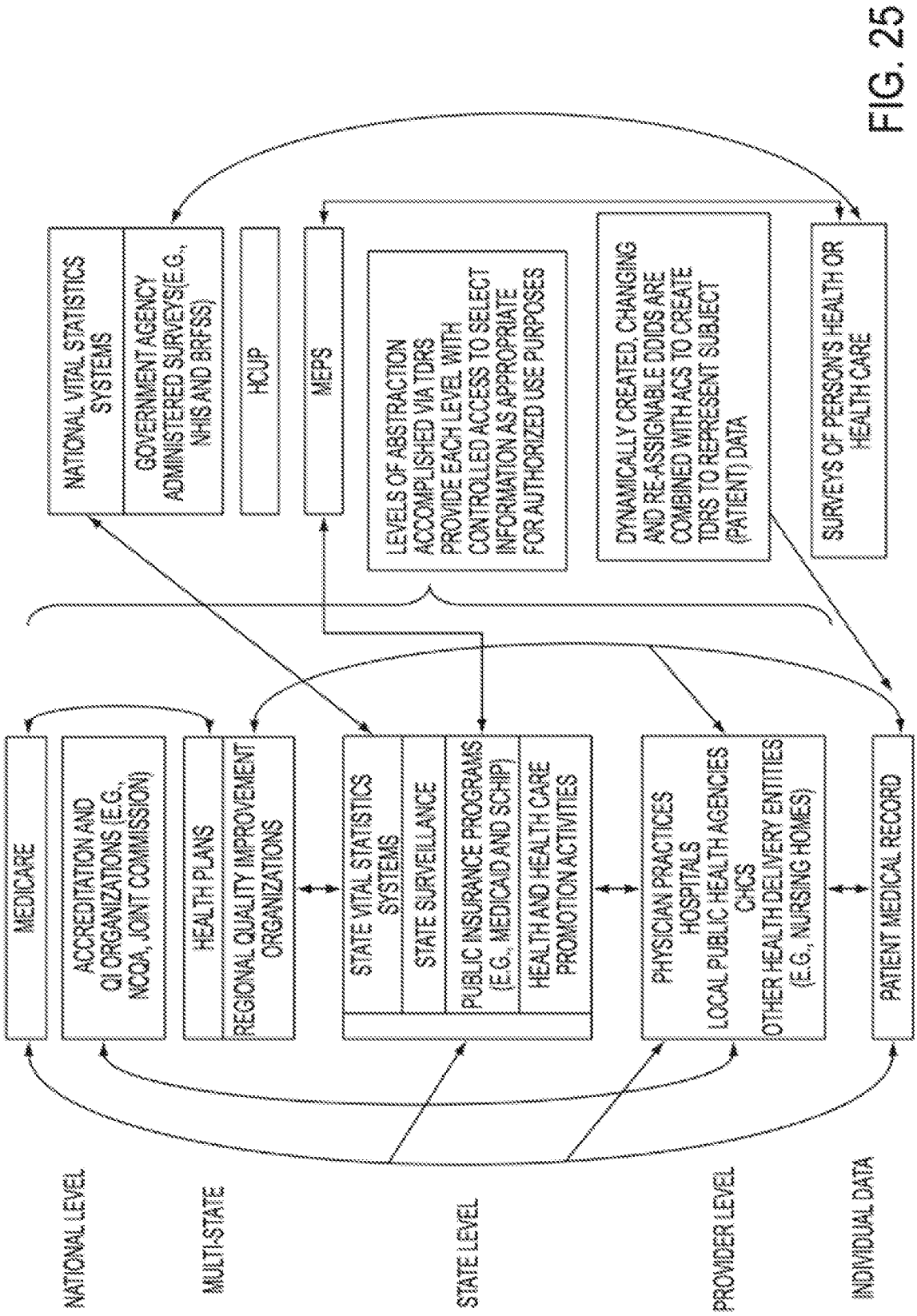

NATIONAL LEVEL
MULTI-STATE
STATE LEVEL
PROVIDER LEVEL
INDIVIDUAL DATA
MEDICARE
ACCREDITATION AND QI ORGANIZATIONS (E.G., NCQA, JOINT COMMISSION)
HEALTH PLANS
REGIONAL QUALITY IMPROVEMENT ORGANIZATIONS
STATE VITAL STATISTICS SYSTEMS
STATE SURVEILLANCE
PUBLIC INSURANCE PROGRAMS (E.G., MEDICAID AND SCHIP)
HEALTH AND HEALTH CARE PROMOTION ACTIVITIES
PHYSICIAN PRACTICES
HOSPITALS
LOCAL PUBLIC HEALTH AGENCIES
CHCS
OTHER HEALTH DELIVERY ENTITIES (E.G., NURSING HOMES)
PATIENT MEDICAL RECORD
NATIONAL VITAL STATISTICS SYSTEMS
GOVERNMENT AGENCY ADMINISTERED SURVEYS(E.G., NHIS AND BRFSS)
HCUP
MEPS
LEVELS OF ABSTRACTION ACCOMPLISHED VIA TDRS PROVIDE EACH LEVEL WITH CONTROLLED ACCESS TO SELECT INFORMATION AS APPROPRIATE FOR AUTHORIZED USE PURPOSES
DYNAMICALLY CREATED, CHANGING AND RE-ASSIGNABLE DDIDS ARE COMBINED WITH ACS TO CREATE TDRS TO REPRESENT SUBJECT (PATIENT) DATA
SURVEYS OF PERSONS HEALTH OR HEALTH CARE

FIG. 25

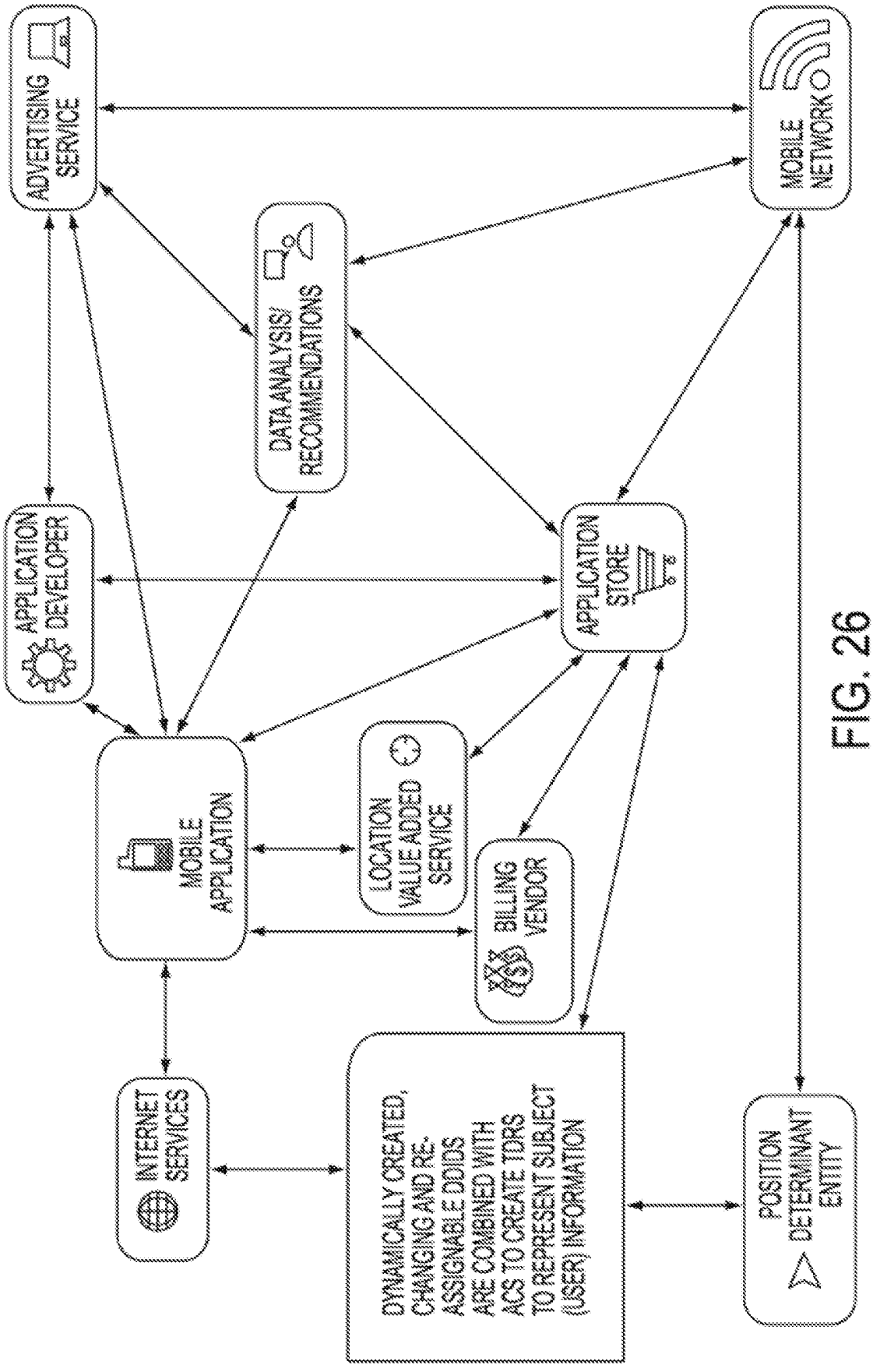

ADVERTISING SERVICE
MOBILE NETWORK
DATA ANALYSIS/ RECOMMENDATIONS
APPLICATION DEVELOPER
APPLICATION STORE
MOBILE APPLICATION
LOCATION VALUE ADDED SERVICE
BILLING VENDOR
INTERNET SERVICES
DYNAMICALLY CREATED, CHANGING AND RE-ASSIGNABLE DOIDS ARE COMBINED WITH ACS TO CREATE TDRS TO REPRESENT SUBJECT (USER) INFORMATION
POSITION DETERMINANT ENTITY

FIG. 26

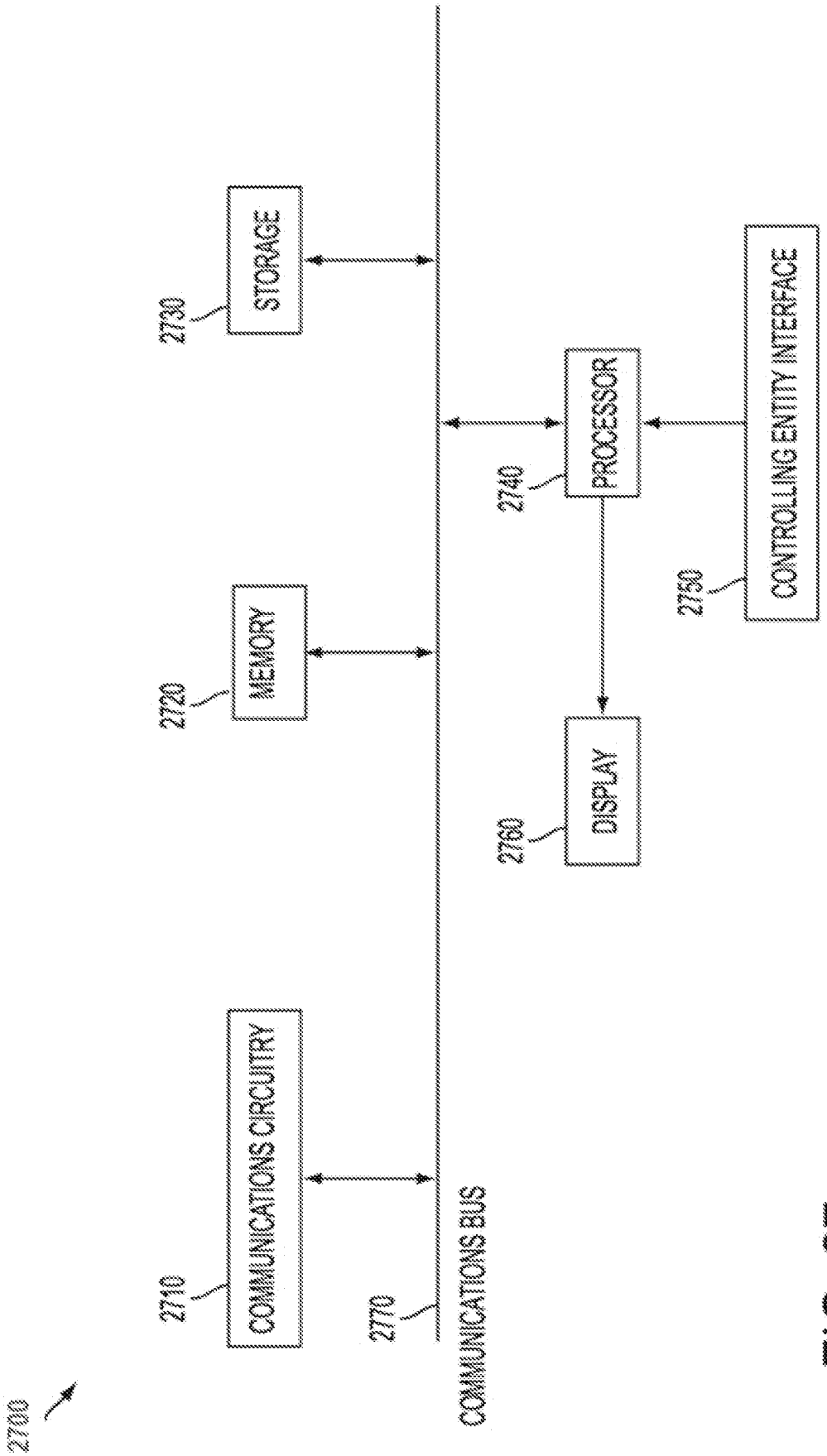

2700
2710
COMMUNICATIONS CIRCUITRY
2720
MEMORY
2730
STORAGE
2740
PROCESSOR
2750
CONTROLLING ENTITY INTERFACE
2760
DISPLAY
2770
COMMUNICATIONS BUS

FIG. 27

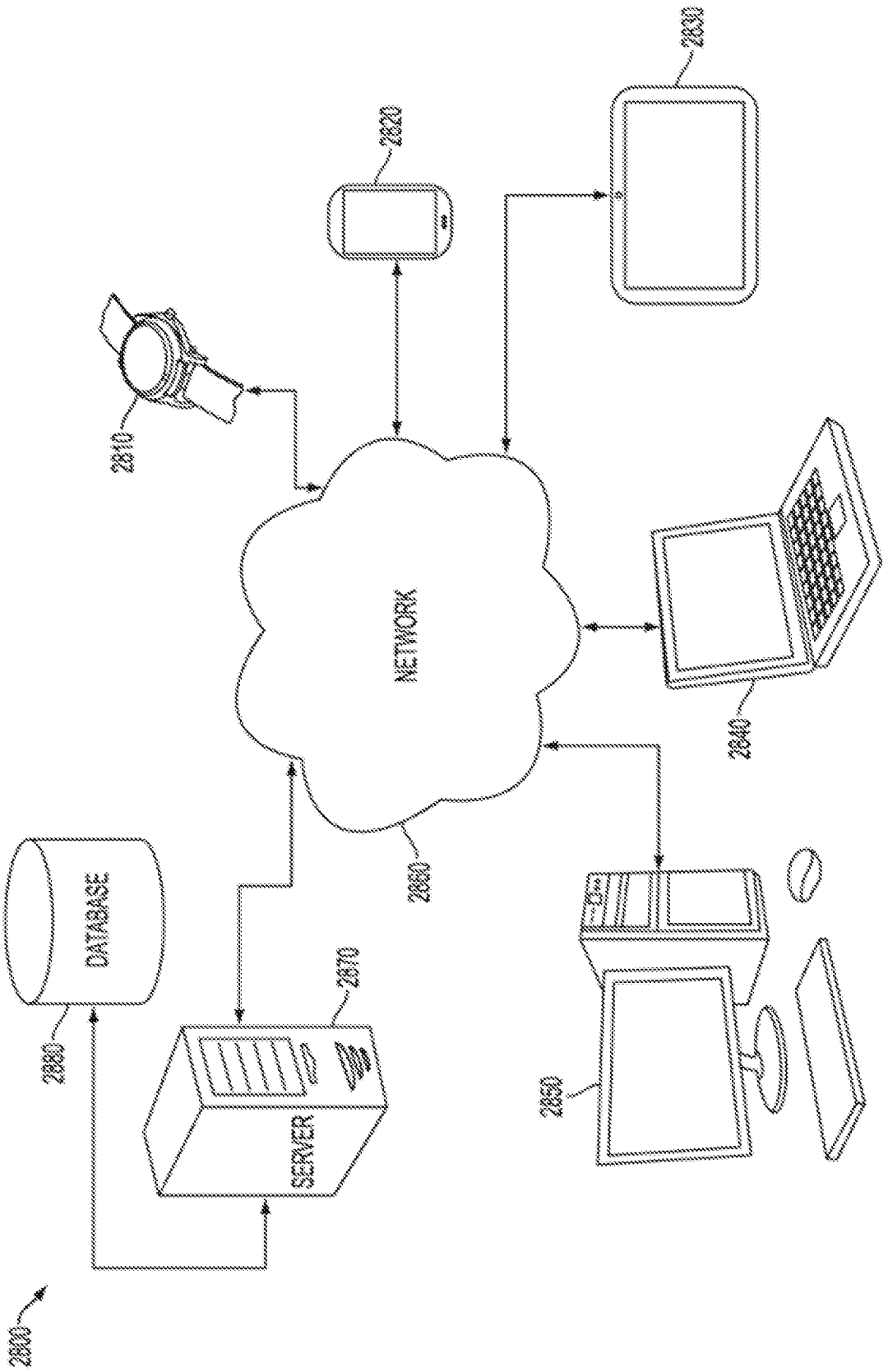

2800
2810
2820
2830
NETWORK
2840
2850
2860
2870
SERVER
2880
DATABASE

FIG. 28

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 20110010563 A1 **[0011]**