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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 April 2017 (13.04.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/062601 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/02* (2009.01)
H04L 29/08 (2006.01) *H04W 4/00* (2009.01)

(21) International Application Number:
PCT/US2016/055719

(22) International Filing Date:
6 October 2016 (06.10.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/239,764 9 October 2015 (09.10.2015) US

(71) Applicant: **INTERDIGITAL TECHNOLOGY CORPORATION** [US/US]; 200 Bellevue Parkway, Suite 300, Wilmington, DE 19803-3727 (US).

(72) Inventors: **LEE, Kuo-Chu**; 30 Revere Court, Princeton Junction, NJ 08550 (US). **LOEB, Shoshana**; 127 West Chestnut Hill Avenue, Philadelphia, PA 19118 (US).

(74) Agents: **ROCCIA, Vincent J.** et al.; Condo Roccia Koptiw LLP, 1800 JFK Blvd., Suite 1700, Philadelphia, PA 19103 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: MULTI-LEVEL DYNAMIC PRIVACY MANAGEMENT IN AN INTERNET OF THINGS ENVIRONMENT WITH MULTIPLE PERSONALIZED SERVICE PROVIDERS

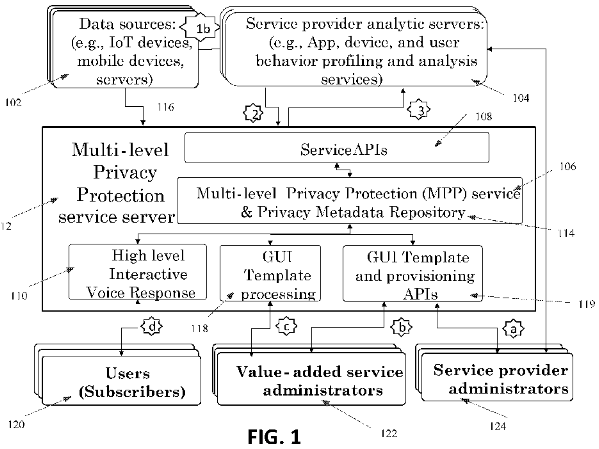

Data sources:
(e.g., IoT devices, mobile devices, servers)
1b
Service provider analytic servers:
(e.g., App, device, and user behavior profiling and analysis services)
102
116
2
3
104
108
Multi-level Privacy Protection service server
ServiceAPIs
106
Multi-level Privacy Protection (MPP) service & Privacy Metadata Repository
112
114
High level Interactive Voice Response
GUI Template processing
GUI Template and provisioning APIs
110
119
d
118
c
b
a
Users (Subscribers)
Value-added service administrators
Service provider administrators
120
122
124

FIG. 1

(57) **Abstract**: Systems, methods, and instrumentalities are disclosed for managing multi-level privacy protection. A first template relating to a first service provider and a second template relating to a second service provider may be received. The first template may include a first and second privacy level, and the second template may include a third and fourth privacy level. Respective privacy levels are associated with respective levels of privacy to maintain for user information. A respective service that is available or that is not available is determined for the respective privacy levels. An indication of the respective service that is available or that is not available for the respective privacy levels is provided. An indication of a respective privacy level to use for a respective service provider is received, and a user interaction with the respective service provider is coordinated. The indicated respective privacy level associated with the respective service provider is maintained.

WO 2017/062601 A1

MULTI-LEVEL DYNAMIC PRIVACY MANAGEMENT IN AN INTERNET OF THINGS ENVIRONMENT WITH MULTIPLE PERSONALIZED SERVICE PROVIDERS

CROSS REFERENCE

[0001] This application claims the benefit of U.S. Provisional Application No. 62/239,764 filed on October 9, 2015, which is incorporated herein by reference as if fully set forth

BACKGROUND

[0002] As the number of personalized services increases (e.g., as smart IoT enabled personalized services increases), protection of statistical data collected from multiple services used in a user profiling process may result in unintended leak or misuse.

SUMMARY

[0003] Systems, methods, and instrumentalities are disclosed for managing multi-level privacy protection. A first template relating to a first service provider and a second template relating to a second service provider may be received. The first template may include a first and second privacy level, and the second template may include a third and fourth privacy level. Respective privacy levels are associated with respective levels of privacy. For example, respective privacy levels are associated with respective levels of privacy to maintain for user information. A respective service that is available, or that is not available, is determined for the respective privacy levels. An indication of the respective service that is available, or that is not available, for the respective privacy levels is provided. An indication of a respective privacy level to use for a respective service provider is received. A user interaction with the respective service provider is coordinated. The indicated respective privacy level associated with the respective service provider is maintained.

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 is a diagram of an example multi-level privacy protection service architecture and work flow.

[0005] FIG. 2 is a diagram of an example multi-level privacy protection service for multiple service providers.

[0006] FIG. 3 is a diagram of an example multi-level privacy control GUI Template.

[0007] FIG. 4 is a table of example service action dependencies on multi-level, multi-stage privacy settings.

[0008] FIG. 5 is a flow chart of an example privacy sensitive personalized service work flow.

[0009] FIG. 6 is a diagram of an example model for estimating the behavior category of anonymous users.

[0010] FIG. 7 is a diagram of an example work flow for estimating scores for user with high privacy protected data.

[0011] FIG. 8 is a diagram of an example multi-level privacy protection service (MPP) sign-on and operation GUI.

[0012] FIG. 9 is a diagram of an example service provider data sharing relationship.

[0013] FIG. 10A is a system diagram of an example communications system in which one or more disclosed embodiments may be implemented.

[0014] FIG. 10B is a system diagram of an example wireless transmit/receive unit (WTRU) that may be used within the communications system illustrated in FIG. 10A.

[0015] FIG. 10C is a system diagram of an example radio access network and an example core network that may be used within the communications system illustrated in FIG. 10A.

[0016] FIG. 10D is a system diagram of another example radio access network and an example core network that may be used within the communications system illustrated in FIG. 10A.

[0017] FIG. 10E is a system diagram of another example radio access network and an example core network that may be used within the communications system illustrated in FIG. 10A.

DETAILED DESCRIPTION

[0018] A detailed description of illustrative embodiments will now be described with reference to the various figures. Although this description provides a detailed example of possible implementations, it should be noted that the details are intended to be exemplary and in no way limit the scope of the application. In addition, the figures may illustrate one or more message charts, which are meant to be exemplary. Other embodiments may be used. The order of the messages may be varied where appropriate. Messages may be omitted if not needed, and, additional messages may be added.

[0019] Service providers may share statistical data to external entities (e.g., business partners, other service providers, etc.). When service providers share statistical data to external entities, the statistical data may include raw data (e.g., de-identified data, anonymized data, etc.). Raw data may be analyzed by statistic methods. De-identified data may include a data set with personal identifiers (e.g., name, social security number, etc.) removed. Anonymized data may include a data set that may have been processed by one or more anonymization processes (e.g., k-anonymity, t-closeness, etc.). For example, anonymized data may include a data set that may have been processed by one or more anonymization processes to add protection on quasi-identifiers (e.g., zip code, age, and/or other information that may be used to re-identify the personal identity). Anonymized data may control the level of protection and/or difficulty needed to re-discover personal identification. Statistical data may include predictive analytic models. For example, statistical data may include predictive analytic models based on the Predictive Model Markup Language (PMML) standard. The service providers and/or third parties may have background knowledge and/or information about the users. For example, the service providers and/or third parties may have background knowledge and/or information about the users from multiple sources. If the raw data and PMML models are shared (e.g., shared freely, shared without the user's consent, etc.), it may be possible to correlate the statistical data from multiple sources and/or discover the identities of users. In some examples, it may be possible to discover the identifies of users with high probability.

[0020] Privacy protection may remove user identity data (e.g., name, SSN and/or address) and/or user privacy control parameters. Privacy protection may be associated with enforcing anonymity of quasi-identities (e.g., area code, age, and/or gender) associated with sensitive information (e.g., medical condition, financial transactions, etc.) before releasing the data. For example, K anonymity may require thresholds for K anonymous users in each quasi-identifier group. l-diversity and t-closeness may require addition constraints on data distribution. Theoretical foundations on differential privacy may add noise to the results of statistical database queries. For example, theoretical foundations on differential privacy may add noise to the results of statistical database queries based on sensitivity levels. Innovative AI inference methods may support dynamic privacy protection for user queries.

[0021] User behavior profiling may comprise collecting, analyzing, and/or categorizing user behavior. For example, user behavior profiling may comprise collecting, analyzing, and/or categorizing user behavior for marketing and customer relationship management. Based on the profiling information, personalized services may be offered to users. For example, based on the profiling information, personalized services may be offered to users at moments of engagements in real-time, which may improve user experiences, system efficiency, and/or reliability.

[0022] Private data may be protected if the data is consolidated in one database and/or controlled by a strict privacy policy on anonymity level for the dataset (e.g., the whole dataset). Theoretical results may be applied to protecting statistical data collected and/or used by user behavior profiling processes in a context sensitive IoT enabled pervasive service environment with multiple service providers. When applying the theoretical results to protecting statistical data collected and/or used by user behavior profiling processes in a context sensitive IoT enabled pervasive service environment with multiple service providers, one or more of the following may occur.

[0023] From the users' perspective, the relationship between the privacy options and/or release of statistical data to business partners may not be revealed to the user. Web sites, browsers, social network, and/or mobile applications may provide different privacy statements and settings that may support (e.g., only support) binary decisions to opt in, or opt out, of a specific privacy protection category (e.g., location, post, chat group, browsing history, the site visited, etc.). The binary privacy options may not be mapped to multiple anonymity levels (e.g., threshold setting for t-closeness, and/or query sensitivity setting for differential privacies).

[0024] From the service providers' perspective, there may be a limited, and/or nonexistent, common privacy control model to support multiple privacy levels when releasing statistical data (e.g., de-identified raw data, PMML model, and/or analysis results, such as scores and actions) to business partners. Business partners may include insourcing, outsourcing, and/or service partners. For example, when one service provider uses t-closeness, the other service provider may use differential privacy. The mapping between privacy levels and/or anonymity control parameters (e.g., threshold setting for t-closeness, and/or query sensitivity setting for differential privacy) may be different between service providers. Service providers may need to provide the anonymity measures to one or more (e.g., each) types of data and/or to develop a mechanism to protect a (e.g., each) type of data separately when the statistical data (e.g., the anonymized data set and/or PMML data) is shared and/or potentially merged by business partners. For example, purchase behavior pattern models, including location and/or items for a small number of users, may need a higher anonymity level than models containing summary behavior from a large number of users. The anonymity control threshold (e.g., t-closeness) based on data distribution model may need to be adjusted. For example, the anonymity control threshold based on data distribution model may need to be adjusted because the data distribution model of combined data set may be different from the original data set.

[0025] Effective privacy protection may consider (e.g., may need to consider) the anonymity levels on multiple types of data and/or an easy to use user interface for a user to set privacy levels for multiple types of statistical data with the understanding of the impacts to the anonymity level and/or trade-offs on the personalized service. For example, a user may not be aware of the meaning of PMML and/or impact of the privacy level settings on anonymity. The user may need to know the impact of anonymity to personalized service and/or service accuracy. Dynamic adjustment of privacy levels (e.g., anonymity level) across multiple applications offered by multiple service providers may introduce complexities in user interfaces and/or trade-offs between anonymity and/or personalize service.

[0026] De-identified and/or anonymized data (e.g., statistical data) may be released and/or shared. Releasing and/or sharing de-identified and/or anonymized data collected and/or used by user behavior profiling processes (e.g., in a context sensitive IoT enabled pervasive service environment with multiple service providers) may result in there being other ways that privacy may be compromised. For example, privacy may be compromised from unintentional leaks and/or intentional investigation. Intentional investigation may include using information obtained outside the application and/or service domains of the service providers. For example, when users choose to reveal different parts of private information based on different contexts (e.g., who, where, when) for one application or service, other applications and services may use this information to derive the behavior patterns and/or discover the identity and sensitive information of the user. To protect user data and/or behavior models, it may be helpful and/or necessary to unify the privacy protection operations.

[0027] Methods, systems, and instrumentalities are disclosed that may enable multiple service providers to share user profiling data to achieve better personalized service actions. Multiple service providers may share user profiling data to achieve better personalized service actions while providing multiple levels of privacy protection based on user preferences. Sharing user profiling data may help service providers gain a broader understanding of user behavior model(s). For example, sharing user profiling data may help service providers gain a broader understanding of user behavior model(s) to offer better personalized services under different contexts. Providing multiple levels of privacy may enable users to change (e.g., increase or lower) the privacy restriction on data collection and/or analysis for service providers. For example, providing multiple levels of privacy may enable users to lower privacy restriction on data collection and/or analysis for service providers that may result in receiving better context sensitive (e.g., location, time, and activities) personalized services. Disclosed implementations may protect privacy of service actions delivered to users, and/or manage feedback(s) from users to improve effectiveness and/or privacy concerns.

[0028] A privacy protection service (e.g., an example multi-level privacy protection service 106, as shown on FIG. 1) may provide better privacy protection when data (e.g., profiling data) from multiple sources are merged by multiple service providers and their partners. By collecting profiling data from multiple service providers, it may be possible to gain a better understanding of combined data distributions. Based on combined data distribution, the anonymity level may be adjusted to reduce unintended leaks. For example, consider two data distribution models collected on a user in two different locations and/or at different times. Merging the two models based on time and location may provide a finer granular context aware distribution model for users in different times and/or places.

[0029] The privacy protection service (e.g., multi-level privacy protection service 106) may check and/or map the privacy levels to control threshold parameters used in one or more anonymity control methods (e.g., K-anonymity, t-closeness, and/or differential privacy). The privacy protection service checking and/or mapping the privacy levels to control threshold parameters used in one or more anonymity control methods may anonymize one or more of data, model, scores, and/or service actions. Detecting data from one or more sources may have intersections that may produce joined results. When detecting data from one or more sources that may have intersections producing joined results, the level of anonymity from the original data may be reduced. For example, when detecting data from one or more sources that may have intersections producing joined results, the level of anonymity from the original data may be reduced and/or the proposed privacy protection service may notify the original service providers for confirmation before releasing the data to business partners and/or users.

[0030] FIG. 1 shows an example system. The example system may comprise one or more of the illustrated features, which may include unified graphical user interfaces (GUIs) and/or application interfaces (APIs) for users (e.g., subscribers) and/or service providers. These may be used to define, configure, and/or manage multi-level privacy protection on the statistical user profiling data and/or the service actions offered to users.

[0031] The privacy level setting may be associated with one or more context sensitive parameters. For example, the privacy level setting may be associated with one or more user activities, application tasks, time, location, and/or other environment conditions. Service providers may define template(s) for a user to specify the privacy levels and/or maximal requirements required for service actions. For example, service providers may define template(s) for a user to specify the privacy levels and/or maximal requirements required for service actions that can be received by the user to protect service actions privacy. Service actions privacy may be denoted as “a” in FIG. 1. Service providers may define constraints on maximum privacy level setting(s) on statistical data. For example, service providers may define constraints on maximum privacy level setting(s) on statistical data to ensure that the accuracy level of anonymized data may be sufficient. For example, service providers may define constraints on maximum privacy level setting(s) on statistical data to ensure that the accuracy level of anonymized data may be sufficient to provide effective personalized service actions. Third party service provider(s) may specify template(s) that may combine multiple services. Multiple services may be denoted as “b” in FIG. 1.

[0032] Templates may be defined and/or provisioned by the administrators and/or stored in the privacy metadata repository. A GUI template processing sub-system may provide an interface for users to access templates created by the service providers and/or the third party value added service providers to the GUI template processing. The GUI template processing may be denoted as “c” in FIG. 1. The GUI template processing may define a privacy preference knowing consequence (e.g., trade-off) of not receiving accurate personalized service based on a maximal privacy level defined in the service action template. A high level user interface (e.g., an interactive voice response (IVR) system, or an intuitive touch-screen based UI) may be provided to support easy to use operations. Easy to use operations may be denoted as “d” in FIG. 1. In some cases, the user interface may be a “hands-free” user interface.

[0033] As shown in FIG. 1, the example system may comprise web service APIs, service processing functions, and/or a privacy metadata repository to receive and/or process statistical data from one or more data sources 102 and/or service providers (e.g., service provider analytic server 104). For example, web service APIs, service processing functions, and/or a privacy metadata repository may receive and/or process statistical data from data sources 102 including IoT devices, mobile devices, and servers. Web service APIs, service processing functions, and/or a privacy metadata repository may receive and/or process statistical data from service provider analytic server 104. Service provider analytic server 104 may include an App, a device, and/or user behavior profiling and/or analysis service providers. The web service APIs, service processing functions, and/or a privacy metadata repository may directly and/or indirectly receive and/or process statistical data from data sources 102 and/or service provider analytics server 104. The proposed system may support the standard PMML statistical data that may comprise typical data mining and/or scoring models including event data set {D} collected from IoT and/or user devices, analytic models, {M} derived from raw data, and/or scores, {S} generated using the input event data and/or the model.

[0034] Users may define different privacy levels. For example, users may define different privacy levels on event data, models, and/or scores for multiple and/or different applications, tasks, activities, locations, and/or times. Multi-level privacy protection may take the user defined privacy levels into consideration when generating anonymized data, {D'}, combined models, {M'}, and/or scores, {S'}, based on the combined model. A privacy protection service (e.g., the example multi-level privacy protection service 106, shown in FIG. 1) may comprise and/or provide one or more multi-level privacy protection service API(s) 108. The multi-level privacy protection service API(s) 108 may process data from multiple data sources and/or return the privacy protected data back to the service provider analytic server 104.

[0035] The anonymized data, model, and/or scores may be shared among service providers. Sharing the anonymized data, model, and/or scores among service providers may provide better privacy preserving personalized services. For example, based on privacy level setting(s) of individual users, a service provider may select higher anonymity thresholds for t-closeness (e.g., to improve privacy) and/or may lower the random noise of differential privacy query (e.g., to improve accuracy, such as utility) of personalized service actions. The privacy aware service actions {SA'i} may depend on one or more privacy aware scores {S'i}.

[0036] The example of FIG. 1 may provide a repository (e.g., privacy metadata repository 114) that may associate privacy level settings for data (e.g., each types of statistical data) with context information. Context information may include application, task, activity, time of the day, and/or location information. The privacy metadata repository 114 may provide GUI and/or service interfaces. The GUI and/or service interfaces may support the development of value added services. For example, the GUI and/or service interfaces may support the development of value added services to optimize service effectiveness and/or privacy concerns. For example, the GUI and/or service interfaces may support the development of value added services to optimize service effectiveness and/or privacy concerns by adjusting service action privacy constraints based on feedback on privacy concerns and/or effectiveness measurements. The privacy metadata repository 114 may provide one or more APIs for service provider(s) and/or value added service provider(s) to define privacy to anonymity level mapping. Privacy levels (e.g., 0, 1, 2, 3, 4, 5) may be mapped to anonymity levels (e.g., 0, 10, 50, 100, 500, 1000). For example, anonymity level values (e.g., each anonymity level value) may represent a number of users, and/or additional users, whose data may be aggregated and/or combined with a first user's data (e.g., in order to meet the privacy level requirement of the first user). The mapping may be accessed by the user such that the user is aware of anonymity levels of statistical data released by the service provider.

[0037] The example system of FIG. 1 may provide a high level user interface to facilitate dynamic setting of privacy levels under different contexts. The high level user interface may be a voice and/or natural language translator. For example, the high level user interface may be a high level interactive voice response (IVR) 110. The high level interface (e.g., high level interactive voice response (IVR) 110) may take inputs from a user and/or extract key words (e.g., privacy level and/or application name(s)). The system may map the key words to the entries in the privacy level setting templates stored in a privacy management metadata repository 114. A user may use a high level natural language interface to define activities and/or set privacy levels for the data generated from one or more applications and/or tasks. For example, a user may like to keep a personal healthcare activity (e.g., rehab, biking, and/or hospitalization) private. The user may want to receive road hazard information services. In this case, the user may interact with the privacy level control interface according to the following example dialog:

User: "Define private activity."
System: "Name the activity or application."

User: "Activity A: Going out." NOTE: examples of a user going out may include the user going on vacation, seeing a specialist, or other place that may reveal duration or types medical conditions.
System: "What is the privacy level for the activity?"

User: "high privacy."
System: "Set all the data from this activity to high privacy."

User: "You may lower the privacy for location service to receive road hazard alerts."
System: "Do you like to set privacy for specific application for this activity?

User: "Lower privacy level on location data to road hazard alert service only."

System: "Your personal identification will not be revealed. However, we will share an anonymized statistical distribution based on location and age for at least 20 anonymized users. Do you want to block the sharing?"

User: "Yes."
System: "High privacy for all other applications and services."

User: "Confirmed privacy settings for "Activity A: Going out""

[0038] A user may adjust the privacy setting for the above example dialogue. In this example, dynamic activation and adjustment of privacy setting for "Activity A: Going out" may be according to the below example dialogue.

User: "Change privacy setting."
System: "what activity or application?"

User: "Activity A: Going out" to medium privacy.:
System: "Ok. Any exceptions:"

User: "Facebook posting."
System: "Ok. Privacy level of activity Going out is lowered to medium, except Facebook posting."
....

[0039] Service provider(s) may provide a default set of privacy settings for a user. The default set of privacy settings may be to simplify the interaction. The service provider may provide privacy level definitions. For example, the service provider may provide privacy level definitions corresponding to k-anonymity, t-closeness, and/or differential privacy control parameters. For example, for Level 5 privacy on data, users may not be distinguishable from at least K = 20 users through quasi-identifiers. Quasi-identifiers may include area code, age, and/or height that may be grouped by the service provider. The example system of FIG. 1 may record the privacy level adjustment patterns for each user. For example, the system may record the privacy level adjustment patterns for each user based on privacy setting examples from other existing users. The system may recommend suitable settings (e.g., may automatically recommend suitable settings).

[0040] A service server (e.g., Multi-level Privacy Protection service server 112) may obtain multiple types of data. For example, the service server may obtain multiple types of data from service providers. The service server may obtain the data through the service API 108. The multi-level privacy protection service server 112 may process data (e.g., multiple types of data). For example, the multi-level privacy protection service server 112 may process data based on the privacy level setting information stored in the privacy metadata repository 114. As shown in

FIG. 2, data (e.g., multiple types of data) received from service providers may be processed by one or more modules. The resulting anonymized raw data set, models, and/or scores may be sent to the service provider (e.g., service provider analytic server 104) and/or may be shared. For example, the resulting anonymized raw data set, models, and/or scores may be shared with business partners. The multi-level privacy protection service may generate privacy protected, context aware actions. For example, the multi-level privacy protection service may generate privacy protected, context aware actions to action service providers. The action service providers may be the service providers and/or partners of the service providers.

[0041] The following describes an example multi-level privacy protection (MPP) service server (e.g., multi-level privacy protection (MPP) service server 112). In an example, shown on FIG. 2, MPP service server 112 may comprise an MPP service 106 and/or a Privacy metadata repository 114. Multi-level privacy protection (MPP) service 106 may be comprised of one or more modules. For example, Multi-level privacy protection (MPP) service 106 may be comprised of a data privacy filter 202, model combination 204, privacy aware scoring 206, context aware actions 208, user privacy control 210, and/or service action privacy control 212, as shown on FIG. 2.

[0042] User privacy control module 210, illustrated in FIG. 2, may provide GUIs and/or APIs for a user and/or a user application to access the user privacy level setting data. For example, user privacy control module 210 may provide GUIs and/or APIs for a user and/or a user application to access the user privacy level setting data stored as a set of multi-level profile data privacy settings. The set of multi-level profile data privacy settings may (e.g., may each) be associated with a user profile data in the privacy metadata repository 114. The privacy setting data may be modeled. For example, the privacy setting data may be modeled using object-oriented design methodology. The privacy setting data may support, create, read, update, and/or delete methods on the privacy level setting data. The set of multi-level profile data privacy settings may contain a context aware privacy protection attribute and/or value pairs for privacy level adjustment under different contexts. Different contexts may include one or more applications, activities, times, and/or locations.

[0043] An example privacy level adjustment template 300 is illustrated in FIG. 3. A subscriber may adjust one or more privacy levels 316 for statistical data (e.g., may adjust privacy levels dynamically). For example, a subscriber may adjust one or more privacy levels 316 for statistical data based on an application, activity, time and/or location. The subscriber may adjust one or more privacy levels 316 for statistical data for each service action. The privacy setting object model may provide methods for one or more users to adjust the privacy level based on context for multiple types of data. For example, the privacy setting object model may provide methods for one or more users to adjust the privacy level based on context for raw data, analytic models, and/or classification scores. The one or more users may adjust the privacy level independently. Attributes may be added to the object model (e.g., may be added to the object model dynamically). Attributes may include links to service actions and/or user groups. The object model may allow users to define and/or adjust privacy settings to engage in service actions of different types based on contexts of interests.

[0044] Dynamic privacy adjustment (e.g., dynamic privacy adjustment based on activities, location, and/or time) may be a function component and/or feature of the example system illustrated in FIG. 2. The template 300, as illustrated in FIG. 3, may be stored in the privacy metadata repository 114. Users and/or systems may set the privacy level setting template 300 using a high level user interface. The user privacy control module 210 may access the privacy setting template 300 stored in the repository 114 and/or automatically select the corresponding privacy setting as the user switches activities and/or uses different applications in different places and/or times. When the user's activity changes, the privacy level settings for one or more (e.g., different) data types (e.g., raw, model, and score) for each applications and/or services may change (e.g., dynamically change) with the activity. The data types may include raw, model, and score. The time and/or location range specifications for activities and/or subtasks (e.g., each activity and/or subtask) within the application may support one or more (e.g., different) privacy settings. The privacy settings may change (e.g., change automatically) as the user moves from place to place. For example, the privacy settings may change as the user moves from place to place at different times.

[0045] Template 300, illustrated in FIG. 3, may be created and/or managed by the user privacy control module 210 of the multi-level privacy protection service 106. For example, template 300 may be created and/or managed by the user privacy control module 210 of the multi-level privacy protection service 106 with inputs pre-populated with one or more default values. The inputs may be pre-populated with one or more default values by administrators for service providers and/or third party value added service providers. The inputs may be pre-populated for each application. The system may generate template 300 for each user with a default privacy level that is equal to, and/or lower than, a privacy level required to receive personalized service for one or more (e.g., each) applications. For example, once the template 300 is configured by the administrators, the system may generate template 300 for each user with a default privacy level that is equal to, and/or lower than, a maximum privacy level required to receive personalized service for one or more applications. Users may click and/or select the privacy level from an option menu. A voice activated script may interact with the user to collect user input and/or populate the template 300. For example, a voice activated script may interact with the user to collect user input and/or populate the template 300 to support hands-free operation.

[0046] As described herein, the template 300 may support PMML based statistical data. The PMML based statistical data may include training raw data, models, and/or scores. The template 300 may provide a data type (e.g., a sample data type) to provide examples to the user about the meaning of a score. The sample data type may include percentile ranking that may be based on a distribution model. The sample data may be defined by a service provider (e.g., service provider analytical server 104) for each application. For example, the sample data may be defined by a service provider to provide detailed meanings of each statistical data that may be shared with business partners. One or more (e.g., additional) user interfaces may be provided for user to click and/or read the meaning of the score and/or business partners who may have access to each type of statistical data. When clicking the privacy level, the user interface may provide the equivalent anonymity levels (e.g., 1 to 1000) for each privacy level (e.g., 0 to 5).

[0047] Service action privacy control 212 may be a function component and/or feature of the example system illustrated in FIG. 2. Service action privacy control 212 may provide GUIs, APIs, functions, and/or object models illustrated in FIG. 4. Service providers may adjust (e.g., dynamically adjust) the privacy levels associated with service actions (e.g., each service actions) for each statistical data type. Additional attributes may be used by service providers to correlate privacy concern rating, and/or effectiveness measurement, with privacy level settings. For example, service action anonymity, effectiveness measurement, and/or privacy concern feedback may be used by service providers to correlate privacy concern rating, and/or effectiveness measurement with privacy level settings. The service provider may be notified to lower the maximal privacy level constraints. For example, the service provider may be notified to lower the maximal privacy level constraints when observing a trend on decreasing user privacy concern feedback and/or increasing effectiveness of a service action. The service provider may be notified to lower the maximal privacy level constraints when observing a trend on decreasing user privacy concern feedback and/or increasing effectiveness of a service action such that the service actions can be offered to an increasing number of users with less privacy concerns on the specific actions.

[0048] The service provider (e.g., service provider analytic server 104) may use a template (e.g., template 300) to configure privacy levels (e.g., maximal privacy levels) for statistical data (e.g., for each type of statistical data, such as PMML training set, model, and/or score). The service provider may use a template to configure privacy levels for service action anonymity privacy levels. The maximal privacy levels may be defined for a user to trade-off the privacy level setting with a personalized service that may be offered. For example, when a user sets a privacy level higher than the maximal level for each types of the data, the data may not be used to provide a personalized service.

[0049] Raw data privacy level may be higher than the maximal raw data privacy level set by the service provider in the template 300. Raw data privacy level may be set by the user. When raw data privacy level is higher than the maximal raw data privacy level set by the service provider (e.g., set by the service provider in the template 300), the user may block one or more service providers from using and/or sharing the raw data. Blocking a service provider from using and/or sharing the raw data may prevent the service provider from using the data collected from the user to generate a model and/or score. Blocking a service provider from using and/or sharing the raw data may be similar to a “do not track” indication from the user. If the raw data is (e.g., is directly) input to and/or processed by the proposed system (e.g. by the Service Server 112, as shown in Fig.1), the proposed system may enforce that raw data is not to be sent to the service provider and/or shared with other service providers. The proposed system may still be able to generate models and scores.

[0050] The model privacy level setting may be higher than the maximal model privacy level set by the service provider. When the model privacy level setting is higher than the maximal model privacy level set by the service provider, the service provider may be restrained from using the privacy protected statistical data to perform scoring (e.g., ranking and/or classification) and/or sharing when the model is generated from a small number of users. When the raw data is processed by the proposed system (e.g., as shown by 116 of FIG. 1), the model may be used to generate one or more scores (e.g., classifications) of users to provide personalized service. The model may be used to generate one or more scores (e.g., classifications) of users to provide personalized service while keeping the model private. For example, the model may be used within the Service Server 112 of FIG.1 to generate scores and/or classifications of users. The model may be used within the Service Server 112 of FIG.1 to generate scores and/or classifications of users without sharing the model to the various service providers. Generating scores and/or classifications of users without sharing the model to the various service providers may enforce privacy while supporting scoring function (e.g., for models containing personal behavior history).

[0051] The scoring privacy level may allow the user to protect specific ranking and classification results from service providers similar to the model. For example, a user may desire to get reward points and/or VIP treatments from a set of interrelated third party providers. For example, a user may desire to get reward points and/or VIP treatments from a game developer (e.g., a developer who offers multiple games) and/or a set of chain stores with business partners. If the user desires to get reward points and/or VIP treatments from a set of interrelated third party providers (e.g., a game developer who offers multiple games and/or a set of chain stores with business partners), the user may permit the service provider to obtain access (e.g., one time access) to score information (e.g., information kept in the privacy metadata repository, e.g., securely kept in the privacy metadata repository). For example, the user may permit the service provider to obtain one time access to score information, which may be information kept (e.g., securely kept) in the privacy metadata repository 114. A GUI may be provided by service provider for user to list and/or click on the partners to authorize the access.

[0052] A privacy metadata repository 114 may be a function component and/or feature of the example system illustrated in FIG. 2. The privacy metadata repository 114 may maintain the object models and/or methods for managing the tradeoff between privacy level (e.g., privacy level of profile data) and/or service effectiveness (e.g., service effectiveness based on contexts shared among service provided by multiple cooperative service providers). The repository 114 may comprise one or more of the following components.

[0053] The repository 114 may comprise an object model for managing raw event data privacy level settings. The object model for managing raw event data privacy level settings may be based on a context. For example, the object model for managing raw event data privacy level settings may be based on one or more application specific contexts, such as vital sign, occupancy, and/or environment behavior data collected by IoT sensors.

[0054] The repository 114 may comprise an object model for managing model privacy level settings of an individual user and/or a group of users. The object model for managing model privacy level settings may be based on application specific contexts. A personal historical behavior model may have higher privacy than the group behavior models.

[0055] The repository 114 may comprise an object model for managing privacy level settings. The object model for managing privacy level settings may be for score. For example, the object model for managing privacy level settings may be for percentile ranking, classification label, etc. The object model for managing privacy level settings may be based on application specific contexts. For some applications (e.g., a desirable ranking, such as a good ranking in academic achievements), a user may want to have lower privacy than in other applications (e.g., medical applications). For example, a user may desire to have a lower privacy for applications relating to a desirable ranking (e.g., a good ranking in academic achievements) than in medical applications.

[0056] The repository 114 may comprise an object model for service action offer constraints on privacy level setting and/or for service anonymity. The service action privacy level setting constraints may provide an understanding of the trade-offs of privacy versus accuracy, availability, and/or relevance of service actions and the privacy level setting. For example, if a user sets a high privacy protection on location, time, and/or activities, then a service provider may not be able to offer services (e.g., real-time location based services) to support the user for specific applications. For example, if a user sets high privacy protection on location, time, and/or activities, then a service provider may not be able to offer services to support the user for specific applications at the moment when the user needs the support. The service action anonymity level setting may be used for protecting the outcome of the user profiling. The service action anonymity level setting may reveal the user preference and/or recent activities. With the service action anonymity feature, users may be willing to modify privacy level settings. For example, with the service action anonymity feature, users may be willing to modify privacy level settings to lower a privacy level setting in return for better services.

[0057] The repository 114 may comprise an object model for tracking effectiveness and/or user rating feedback. For example, the repository 114 may comprise an object model for tracking effectiveness and/or user rating feedback for each application, user activity, location, time, and/or environment conditions.

[0058] An object model may have an application specific privacy level associated with one or more anonymity control parameters. The one or more anonymity control parameters may be used in different types of privacy protection methods. For example, privacy level X (e.g., where X is from 1 to 5) to K-anonymity mapping (PLKA) may be defined as: $\{(X, K)\} = \{(0, 1), (1, 10) (2, 50), (3, 100), (4: 500), (5, 1000)\}$; privacy level to t-closeness mapping (PLTC) may be defined as: $t = 0.05 + X*0.05\}$, t may be default to 0.2; privacy level to Differential-Privacy mapping (PLDP) may be defined as: $S/\epsilon * X/5\}$. S and ϵ may be adjustable sensitivity and/or coefficients that may be set. For example, S and ϵ may be adjustable sensitivity and/or coefficients that may be set based on specific queries to the privacy protected data sets. Other application specific mappings may be defined by service providers. The privacy level to anonymity protection parameter mappings may enable the service provider to adjust the anonymity protection parameter. For example, the privacy level to anonymity protection parameter mappings may enable the service provider to adjust the anonymity protection parameter based on a user defined privacy level. A user may obtain information. For example, a user may obtain information about what types of privacy protection methods are used and/or how many other users are un-distinguishably grouped by quasi-identifiers.

[0059] As shown in FIG. 2, multi-level privacy protection (MPP) service 106 may include a data privacy filter 202, model combination 204, and/or privacy aware scoring modules 206. MPP service 106 may use the privacy level setting stored in metadata repository 114 to control the privacy levels of multiple applications and/or services based on the context (e.g., activity). The input, output, and/or function of each module may be as described herein.

[0060] A data privacy filter 202 may include input(s), function(s), and/or output(s). The inputs may include one or more of the following. For example, the inputs may include an event (e.g., events from multiple sources). The inputs may include privacy level setting(s), such as privacy level settings on event data for each user. The privacy level settings on event data for each user may be under different contexts from metadata repository. The inputs may include privacy level mapping methods (e.g., PLKA , PLTC, and/or PLDP).

[0061] The functions may include one or more of the following. For example, the functions may include a marking privacy level on an (e.g., each) event data set {D}. The marking privacy level on an event data set {D} may be based on the privacy level settings. The functions may include a merging privacy marked data set of the same types (e.g., application, user, privacy setting, and/or contexts) from privacy marked data sets. The functions may include applying PLKA, PLTC, and/or PLDP methods to sensitive data attributers. For example, the functions may include applying PLKA, PLTC, and/or PLDP methods to sensitive data attributers to create anonymized data sets based on privacy level. For example, to achieve 10 anonymity, the PLKA function may scan the merged data set and/or adjust the range of quasi-identifiers. The functions may include using PLTC to check the t-closeness based on the distribution and/or adjusting the K-anonymity dataset. The functions may include verifying and de-identifying confidential attributes (e.g., user identity). The functions may include applying application specific processing (e.g., other application specific processing), to join two data set based on IoT and/or user IDs. The functions may include creating de-identification verified and/or anonymized data sets, {D'}.

[0062] Outputs may include one or more of the following. For example, outputs may include sending {D'} and/or a service entry point to access the anonymized data sets {D'} to service providers.

[0063] Model combination (e.g., combined model generation) module 204, shown in FIG. 2, may include inputs, functions, and/or outputs. The inputs may include one or more of the following models, {M}, from one or more service providers. The model may be a user behavior pattern. For example, the model may be an application usage based on different contexts (e.g., time and/or location). For example, the model may be the spending pattern of users used to decide whether a user should be awarded VIP status; a privacy setting for models from metadata repository; and/or privacy level mapping methods for models from metadata repository. Privacy level mapping methods may include PLKA, PLTC, and/or PLDP for each model. The functions may include one or more of the following. A function may include checking a privacy level setting to the model. Different privacy levels for models derived from each user's personal behavior history may be set by the user to protect the anonymity level when releasing the model to selected applications and/or sub-tasks under one or more (e.g., different) contexts. Contexts may include activity 306, location 314, and/or time 312, as illustrated in FIG. 3. The model may have restricted access for specific applications under the specific context. The service actions privacy control template 400, illustrated in FIG. 4, may have privacy level settings on a service action. The privacy level settings may be predicated on the user behavior model. A service action may be triggered by detecting behavior patterns based on quasi-identifier information description metadata associated with the personal behavior model. The quasi-identifier may include activities, location, time, demographic, and/or preference. A model for a large collection of users may be marked by the service provider. For example, a model for a large collection of users may be marked by the service provider to protect group privacy. The sample data set (e.g., training set) used to derive the model may be provided with the model. For example, a VIP group behavior model may have skewed (e.g., area code) distribution. The service provider may set high privacy levels on area code when sharing the model with other service providers.

[0064] A function may include saving the input model to the data repository. A function may include selecting models from the repository that matches the type of the input model. A function may include combining the models into a new model set $\{M_{i+1}\} = \{M_i, M_{i-1}, \dots M_{i-j-1}\}$ for a window of "j" models. Service provider may choose different statistical methods to merge the models. For example, service provider may choose different statistical methods to merge the models to obtain broader knowledge of data distribution and/or to observe the variation of behavior models under different contexts. Models may be merged and/or linked. For example, models may be merged and/or linked based on context such as location, time, application, and/or user groups. Models derived from the same context for the same user group may be merged using statistical methods for each type of model. For a normal distribution model, the weighted average and/or variance may be calculated. For clustering models, centroids from multiple clusters may be adjusted using various statistical methods. Models derived from different contexts may be linked for one or more users such that as the context changes different models may be used to score the real-time user behavior. A function may include verifying and/or de-identifying confidential attributes. A function may include applying default and/or model specific anonymity protection methods to add noise to the model coefficients (e.g., shifting centroid location, adding standard deviation, and/or reducing precision on decision tree branch conditions). The privacy protection may reduce the model utility. The noise levels added to the models may be revealed to the consuming service providers. A function may include creating anonymized combined model sets {M'}. A function may include saving {M'} in data repository. Outputs may include sending {M'} and/or a service entry point to access the anonymized data sets {M'} to service providers.

[0065] Privacy aware scoring may compare real-time user behavior data with the distribution models. For example, a user's spending and/or visiting frequency to a particular application and/or a physical shop may be scored against the distribution model. The user's spending and/or visiting frequency to a particular application and/or a physical shop may be scored against the distribution model to generate percentile ranking and/or a classification as low, medium, and/or a VIP category. The real-time data may be used to predict the behavior of a user based on a model trained using historical data. Privacy aware scoring may include inputs, functions, and/or outputs. The inputs may include one or more of the following. For example, inputs may include input event data from data set {D'} and/or from external score data set {S}. Inputs may include input Models, {M'}, from the data repository. Inputs may include privacy setting for scores from metadata repository. Inputs may include privacy level mapping methods (e.g., PLKA, PLTC, and/or PLDP) for each model from the metadata repository (such as privacy metadata repository 114).

[0066] The functions may include one or more of the following. As shown in FIG. 2, the privacy aware scoring function 206 may take input score data {S} from the external analytic process and/or apply privacy protection setting to the score data set. The privacy aware scoring function 206 may generate the score data sets based on input data set {D'} collected from the external data source and/or the models {M'} derived by the combined model generation function. A function may include taking external generated score data set {S} and/or scoring the input data {D'} against the model {M'} to generate {S'}. A function may include marking the privacy level setting to {S'}. A function may include applying privacy level protection methods (e.g., PLKA, PLTC, and/or PLDP) to score data set {S'}. A function may include saving the score data set {S'} into the metadata repository. Outputs may include sending {S'} and/or a service entry point to access the anonymized data sets {S'} to service providers.

[0067] Context aware actions may include inputs, functions, and/or outputs. The inputs may include one or more of the following: scores {S'}; privacy setting for service actions from metadata repository (e.g., privacy metadata repository 114); and/or privacy level mapping methods (e.g., PLKA, PLTC, and/or PLDP) for each model from the metadata repository. Functions may include one or more of the following. For example, functions may include marking the service action with the privacy level setting. Functions may include granting privacy permission to the service action (e.g., mark privacy checked) if the input privacy level of the score is lower than the required privacy level constraints specified for the service action (e.g., the accuracy of score is acceptable for the service action). Functions may include applying privacy level mapping methods to the set of service actions, {SA'}. Outputs may include sending {SA'} and/or a service entry point to access the anonymized data sets {SA'} to service providers.

[0068] A model may include types. One type may be built from historical data (e.g., data of one or more users). The model may reveal a summary of user behavior that may be private (e.g., highly private). A user may desire to specify the privacy level associated with such data and/or the service provider may protect sharing of quasi-identifier historical behavior and/or preferences. For models derived from a large number of sample user data, the privacy level setting from the user may be used. For example, the privacy level setting from the user may be used to filter out the user from being included in the sample data set and/or to add noise (e.g., a high level of noise). Filtering out the user from being included in the sample data set and/or adding noise may increase anonymity of quasi-identifiers associated with the model. The proposed system may check the differences in sample data distribution models from multiple service providers. The proposed system may suggest changes to the anonymity control parameters (e.g., t-closeness threshold and/or sensitivity of differential privacy) to the originating service providers.

[0069] Scores may provide ranking of one or more users. The scores of de-identified users may be associated with quasi-identifiers. For example, the scores of de-identified users may be associated with quasi-identifiers such that the statistical distribution and/or classification may be applied and/or used for different business purposes. When sharing scores among service providers, anonymity protection may be applied. For example, anonymity protection may be applied to avoid a privacy leak of information through the quasi-identifiers (e.g., area code, age, presence-location association, etc.). Information may include sensitive information, special interest information, medical condition information, etc. Multiple privacy levels may provide advantages for scores, models, and/or raw data.

[0070] Releasing statistical data may not reveal an identity (e.g., personal identity). Service providers may use the quasi-identifier to learn the customer segmentation beyond the data set that each individual obtains. With more knowledge of customer segmentation based on behavior profile, service provider may develop a more efficient strategy to customer segmentations.

[0071] The multi-level privacy protection service 106 may guard the user from lowering privacy to one or more services (e.g., all services) under one or more contexts (e.g., all contexts). For example, as illustrated in FIG. 3, once the multi-privacy template 300 is set using a high level user interface, the user may be protected from lowering privacy without specific benefits of obtaining better service actions, as illustrated in FIG. 4. The proposed system may prevent service providers from releasing user information. For example, the proposed system may prevent service providers from releasing user information to other service providers unconditionally, or based on a condition. For example, a user may increase privacy of a social network post during vacation to a special remote location for a period of time. If the social network were to share the information to business partners (e.g., after de-identifying the user's identity), the privacy control service may determine if the anonymity criteria for quasi-identifier (e.g. location and/or time) is met before granting the release of the statistical data set that may reveal that the user is away from home (e.g., away from home for a long period of time). Without the protection, there may be a possibility for other service providers to identify the user based on originating location, vacation location, the date of travel, and/or other background information.

[0072] Value-added services, as shown in FIG. 2, may be described herein. The multi-level privacy protection service may provide API and GUI interfaces, as described in FIG. 1. For example, the multi-level privacy protection service may provide API and GUI interfaces to support value-added privacy services for users and/or service providers. Examples may be provided herein to illustrate how different value added service(s) may be implemented by the multi-level privacy protection service.

[0073] Support for privacy level setting and/or enabling service actions based on privacy constraints may be provided. This may include one or more of the following.

[0074] As illustrated in FIG. 5, users and/or administrators 502 may, at 504, enter the privacy setting for statistical data, maximal service privacy level (PL) requirements, and/or the privacy level for service actions. At 506, the value added service may collect usage time (UT) data and/or, at 508, check if the privacy setting is lower than the Max (D). If the privacy level is lower, the processing may, at 510, continue to build the model. At 512, the model privacy protection level may be compared with the maximal privacy level required to use the model. If the privacy level set by the user is lower, the model may, at 514, be used to score the inputs. For example, a user may decide not to reveal any usage time on a game (e.g., during office hours). , The user may not reveal any usage time on a game by setting a higher scoring privacy level (e.g., Pl(UT.S) = 5) than the maximal service privacy level requirements, MaxPL(D | M |S) (e.g., default to level 3 for data, model, and score). As a result, a user may not receive any service action notifications from the game (e.g., during office hours). The user may set higher score privacy and/or leave the data and/or model privacy lower. For example, the user may set higher score privacy and/or leave the data and/or model privacy lower to allow for continued processing of the data and/or model and/or create scores. The scores may be queued in data repository and/or released. For example, the scores may be queued in data repository and/or released when the privacy level for a score is reset (e.g., reset to low) and/or when an on-demand score release is authorized by the user. Service providers and/or business partners may be aware of the privacy setting from the data repository and/or refrain from sending any notifications to the user (e.g., during office hours).

[0075] The user may change score data privacy settings (e.g., during lunch hour). For example, the user may change score data privacy settings to medium level. Changing score data privacy settings to medium level may allow the user to receive some notifications (e.g., notifications of bonuses, promotions, etc.). When the privacy level for the score is lowered (e.g., after work), the queued scores may be released and/or multiple service actions may be triggered. During the weekend, the user may lower the privacy to the lowest level and/or receive the service actions (e.g. all service actions). Business partners may receive data sets with lower privacy levels. For example, business partners may receive data sets with lower privacy levels that may be used to provide personalized services to the user (e.g., when the user is playing a new game). Personalized services may include providing a coupon and/or bonus points to the user. The user may set a high privacy level setting for play time models. For example, the user may set a high privacy level setting for play time models, such that no other business partners may know the player's play time pattern and/or release scores on demand (e.g., to get bonuses and/or rewards).

[0076] A value added service for improving service action accuracy while maintaining high privacy may be provided. This may include one or more of the following.

[0077] When setting a higher level privacy level setting to the data and/or the model, the number of anonymous users may increase and/or decrease. For example, when the number of anonymous users increases, the accuracy (e.g., utility) of the data and/or model may decrease. The accuracy of the data and/or model may decrease for many reasons. One reason the accuracy of the data and/or model may decrease may be because it may be more difficult to identify the classification scores of the anonymous users against distribution models. It may be desirable for service providers to monitor the level of anonymity. For example, it may be desirable for service providers to monitor the level of anonymity when using the shared data and/or models to decide if targeted service action may be effective. FIG. 6 illustrates an example relationship between a privacy level and a number of anonymous users in a multi-dimensional space. For example, FIG. 6 illustrates an example relationship between a privacy level and a number of anonymous users in a multi-dimensional space that may comprise an anonymized data set. The anonymized data set may be collected from users engaging in one or more applications that may support one or more activities in different contexts (e.g., location, time, and/or environment conditions). A user Ui may be engaging in activities (e.g., three different activities) in sequence from time t1 602, t2 604, to t3 606 using one or more applications. The service providers for each application may monitor the behavior of the user Ui using one or more distribution models. For example, service providers for each application may monitor the behavior of the user Ui using three different distribution models (e.g., M1 608, M2 610, and/or M3 612). A user Ui (e.g., a single user Ui) may be engaging at a first activity (e.g., provided by a first service provider) at time t1 602. The first service provider may monitor the user's behavior using model M1 608. At time t2 604, the user may engage in a second activity (e.g., provided by a second service provider), who may use model M2 610 to model the user. At time t3 606, the user may engage in a third activity (e.g., provided by a third service provider), who may use model M3 612 to model the user. The circle around Ui may provide a conceptual model for the number of users in the same anonymous group (e.g., the same group as the Ui). The users may have a same and/or different privacy level settings on the score data {S}. For example, user Ui may set score privacy level 1 for M1 608, 3 for M2 610, and 5 for M3 612, respectively. Privacy level may be correlated with anonymity level. For example, the higher the privacy level, the higher the anonymity level may be, and the more users that may be in the same anonymous group represented within the circle. The cost of service action may increase. For example, the cost of service action may increase because the accuracy may decrease.

[0078] The user may set the privacy level based on an anonymity mapping. For example, the user may set the privacy level based on an anonymity mapping that may be retrieved from a repository (e.g., Privacy metadata repository 114) and/or displayed in the template GUI 300, shown in FIG. 3. The user may refer to the maximal service privacy requirement in FIG. 4 and/or the user may use the default value to obtain medium anonymity while receiving the personalized services. The template may contain sample data descriptors which may describe the model defined by the service provider(s). Users may not need to know the model and/or scoring method to set the privacy level. Users may need to know whether the raw data set of the model may contain sensitive behavior patterns. Sensitive behavior patterns may include a purchasing record with location information, doctor visits, and/or video game player time. For example, a usage time and/or play time pattern model may be easy for users to understand and/or decide what level of anonymity (e.g., 10 or 100) may be sufficient under different contexts.

[0079] To alleviate the cost and/or inaccuracy that may be caused by high anonymity, the proposed system may enable service providers to share behavior models. For example, the proposed system may enable service providers to share behavior models collected from a large population of users with low privacy settings. As the population increases, the distribution model may be more accurate. For example, as the population increases, the distribution model may be more accurate to apply t-closeness measure(s) after defining the anonymity level. The service provider(s) receiving the models from larger population(s) may score the behavior of the users, trigger the service actions, and/or collect effectiveness and/or privacy concern rating feedback from users with predefined privacy settings (e.g., high privacy settings). The effectiveness and/or privacy concern ratings may be measured. For example, the effectiveness and/or privacy concern ratings may be measured to determine if the shared models improve the service action accuracy and/or reduce the cost. To protect the service anonymity, the users may be filtered. For example, users that have low effectiveness and/or high privacy concern rating may be filtered. Users may be filtered by increasing the anonymity level for the service action. For example, the value added service provider may set the service action anonymity level by setting the privacy level setting to 2 and/or by offering a service action (e.g., advertisement) to a set of users with playing time less than 10 days and/or players who spent less than the average users in purchasing virtual goods. Some of the users may prefer not to get the advertisement, and/or may complain that the ads (e.g. contents of the ads) reflect recent activities that the user may consider private. These users may provide a low privacy rating feedback after receiving the advertisements. These users (e.g., some, or all, of these users) may not have increased their spending related the advertised items. The value added service provider may increase the anonymity level by increasing the privacy level (e.g., setting the privacy level to 3).

[0080] The service action anonymity level implemented by a service provider may increase the confidence level for users. For example, knowing that the service action may be provided in a way that is private to the user, the service action anonymity level implemented by a service provider may increase the confidence level for users to lower the privacy level setting. For example, service providers may ensure that service actions are offered to users (e.g., groups of users, such as where the group sizes are large enough to meet the anonymity constraints). If service providers ensure that service actions are offered to users, the users may use low and/or medium privacy levels of statistical data (e.g., in return for receiving more service actions).

[0081] The proposed system may collect user feedback on effectiveness of service actions and/or privacy concerns. For example, the proposed system may collect user feedback on effectiveness of service actions and/or privacy concerns to adjust the privacy constraints of service actions. For example, when users receive a service action (e.g., a service call, promotion, and/or warning) that is not useful to the user and/or that may have revealed private knowledge about the user (e.g., advertisement) that should have been protected, the user may provide privacy concern feedback with a low rating (e.g., rating “1”) and low effectiveness (e.g., effectiveness rating 1) on the service action, respectively. The following rules illustrates how the privacy metadata provided by the system may be used to provide various application specific privacy and/or personalized service action trade-offs. For example, the following rules illustrate how the privacy metadata provided by the system may be used to provide various application specific privacy and/or personalized service action trade-offs effectively. Users, for example, may set the following one or more privacy policy rules to adjust and/or trade-off privacy for personalized service actions. For example, a user may set up one or more of the following rules.

[0082] The following rule may illustrate how the privacy metadata provided by the system may be used to provide various application specific privacy and/or personalized service action trade-offs effectively. If (AppX_Service_Action_Data_Privacy_Requirement = X), then, set (User_AppX_Data_PrivacyLevel to (X-1) for Activity_A1 during weekend and Activity_A2 during weekday). This rule may be defined (e.g., predefined) by value added service providers such that the user may only need to click, select, and/or set the attribute and value pairs {AppX: APP ID, Service_Action_Data_Privacy_Requirement: X}, {User_App: X, Data_PrivacyLevel: X-1} , {Activity1: A1, time_window: {T1, T2}, Activity2: A2, time_window:{T1, T2}. A simple voice response script may be created to collect the value for attribute value pairs. Similar rules may be defined for other parameters in the service action privacy control template. The rules can monitor entries (e.g., rating of privacy concern of a service action in the service provider's action privacy control template) such that value added service provider may turn on and/or off and/or change entry in the template as the service provider changes the service action privacy control policies.

[0083] The proposed system may support service providers to provision service action effectiveness and/or privacy improvement rules. For example, the proposed system may support service providers to provision service action effectiveness and/or privacy improvement rules dynamically. For example, the following rule may implement one or more methods to adjust the service action privacy constraints and/or anonymity based on user feedback. If RatingOfPrivacyConcern(ServiceActionX) > 4 (e.g., the user has medium-high concern on service action X), then perform one or more of the following. If effectiveness(ServiceActionX) < 3, then, increment(PrivacyContraint) (e.g., if the service action is not considered very effective, increase service action privacy constraints on statistical data). If effectiveness(ServiceActionX) > 4 and CostLevel = low (e.g., the cost of the service action is low), then, increment(ServiceActionAnonymity) (e.g., increase the service action anonymity and provide service action to more users if the service action is effective and the cost of the service action is low).

[0084] The proposed system may provide an additional value added service to improve the accuracy of one or more scores. For example, the proposed system may provide additional value added service to improve the accuracy of one or more scores for users who have high privacy settings that may prevent the users from receiving accurate service actions. An estimation of the behavior event data of the target user may be used to replace the protected high privacy data (e.g., which may have high level noise) to compute the score against selected behavior model. The scores may be used to invoke a set of service actions to segments of users grouped by quasi-identifier and/or behavior scores. As illustrated in FIG. 7, when the profiling data for a particular user is protected and/or has privacy level settings higher than the privacy setting constraints (e.g., maximal privacy setting constraints required by a service action), the system may use the context aware effectiveness and/or privacy concern feedback from other users who have similar profile data in the past and/or who are engaged (e.g., currently engaged) in a similar application, activity, and/or context (e.g., location, time, and/or environment condition). The set of service actions received by the set of users who are similar in behavior and/or context may be analyzed by one or more (e.g., different) analysis methods implemented by one or more (e.g., different) service providers. The analysis service may include an association rule, nearest neighbor clustering, and/or a correlation based on a set of inputs selected based on contexts tracked in the data repository.

[0085] To improve the accuracy for users that may set high score privacy, the value added service may select P numbers of users (e.g., users with lower score privacy levels) within the proximity of the Ui from the repository based on highly dependent (e.g., high correlation and/or association) variables discovered from raw data and/or behavior model between Ui and/or the selected user. These variables may be identified by value added service providers using data mining methods and/or used in the selection criteria. Example variables that may be discovered for the proximity selection criteria may include context (e.g., application, location, and/or time), application specific attributes (e.g., skill level, play time, and/or monthly spending), and/or quasi-identifiers (e.g., age, height, and/or school).

[0086] The effectiveness of the variable identified for proximity search may be evaluated by the service provider. For example, the effectiveness of the variable identified for proximity search may be evaluated by the service provider using effectiveness measurement of service actions. If there are no improvement on effectiveness of service actions using the users selected by the proximity search variables, the system may compare the effectiveness of different variables using multiple runs of experiments. For example, users may be informed that to improve personalized service it may be necessary to lower the privacy level.

[0087] APIs for receiving notifications events and/or setting the entries in the privacy control template may be provided. A list of APIs interface description are provided herein.

[0088] Multiple APIs may be supported for subscribers (e.g., users) and/or service providers to adjust privacy level control templates for user and/or service actions, respectively. A summary of APIs that may support the provisioning of dynamic privacy level control templates is provided herein.

[0089] A subscriber GUI and/or API may be an API that supports the provisioning of dynamic privacy level control templates. A subscriber GUI and/or API may perform one or more of the following. For example, a subscriber GUI and/or API may create a privacy control template for a new user. A subscriber GUI and/or API may create entries in a privacy control template for a list of applications offered by service providers. A subscriber GUI and/or API may refresh and/or display application data, model, and score. A subscriber GUI and/or API may display the maximal service action privacy level requirement thresholds. The model and/or score may be listed in the templates with default privacy levels and/or sample data descriptions. For example, the model and/or score may be listed in the templates with default privacy levels and/or sample data descriptions for each model and/or score. The privacy level to anonymity level mapping may be provided as options for users to protect the behavior history model, ranking, and/or classification scores; create activities and/or privacy setting entry for one or more context variables (e.g., location, time, and/or other application specific special events or environment conditions; deploy the automatic privacy adjustment template to privacy metadata repository; subscribe to notifications services for privacy alerts; subscribe to service actions and/or disable service actions; provide privacy concerns rating feedback and/or effectiveness feedback, on-receiving alert or service actions; and/or adjust the privacy levels in the automated privacy control template.

[0090] A subscriber privacy control template monitoring and/or adjustment rule API may be an API that supports the provisioning of dynamic privacy level control templates. A subscriber privacy control template monitoring and/or adjustment rule may perform one or more of the following. A subscriber privacy control template monitoring and/or adjustment rule may create a rule template. A subscriber privacy control template monitoring and/or adjustment rule may list available privacy control variables and/or notification events. A subscriber privacy control template monitoring and/or adjustment rule may list an available API to monitor and/or set entries in service action privacy control template and/or the user privacy control template. A subscriber privacy control template monitoring and/or adjustment rule may define event patterns and/or actions to monitor and set the variables in the templates.

[0091] A service provider service action privacy control template GUI and/or API may be an API that supports the provisioning of dynamic privacy level control templates. A service provider may provision the service action control template similar to the user privacy control template. A service provider may perform one or more of the following. For example, a service provider may create a service action privacy control template for a new application or service. A service provider may create and/or update one or more of the following entries in service action privacy template. A service provider may create and/or update a service action privacy level for raw data, model, and/or score. A service provider may create and/or update a service action anonymity level setting to protect user privacy (e.g. to prevent user’s sensitive data from being revealed by service actions such as special interest purchases, awards, and/or advertisements indicating medical conditions). A service provider may create and/or update a user rating on privacy concern caused by the service action. A service provider may create and/or update a user rating on effectiveness of the service action. A service provider may list statistical distribution of user privacy setting. A service provider may drill down to an individual user privacy control template. A service provider may deploy the service action privacy control template to privacy metadata repository. A service provider may subscribe to notification services for privacy rating and feedback alerts. A service provider may adjust the privacy levels based on user feedback on privacy rating and effectiveness.

[0092] A subscriber privacy adjustment rule API may be an API that may support the provisioning of dynamic privacy level control templates. Subscriber Privacy adjustment rules may create a rule template. Subscriber Privacy adjustment rules may list an available API to monitor and set entries in both service action privacy control template and the user privacy control template. Subscriber Privacy adjustment rules may define event patterns and/or actions (e.g., to monitor user feedback to adjust the service action anonymity level in the service action control templates).

[0093] The GUI and/or API for templates and/or rules may support 3rd party privacy services deployed in servers running in the Cloud and/or private data center. The rule execution may be implemented in one or more types of rule engines and/or software (e.g., proprietary software). The one or more types of rule engines and/or software may be running in servers. The templates may be stored in the scalable privacy metadata repository. The privacy metadata repository may provide service interfaces for one or more rule execution servers.

[0094] Easy to use GUI and/or privacy service cooperation examples may be described. GUI interfaces may be provided using the attribute value-pairs to describe the entries in FIG. 3 and/or FIG. 4. For example, for applications (e.g., every new application) enabled by the privacy service protection service, developers (e.g., application developers) may provide the attribute and/or value pair (e.g., the attribute and/or value pair for each entry). For example, some applications may have finer grain control for privacy based on time and/or location, and/or others may be based on location. The template may comprise all the attribute and/or value pairs from the application and/or service providers that may be used (e.g., used by scripts, such as HTML5 scripts) and/or other types of programs (e.g., GUI programs) to display and/or collect user input (e.g., using menu options). A voice response system function, as shown in FIG. 1, may be used to access the attribute-value pair data structure. For example, a voice response system function may be used to access the attribute-value pair data structure using Web service APIs. The data repository may provide APIs to support the Web services and/or GUI backend logics to select application traversing the time, space, and/or context attribute-value pairs that may be stored in the repository.

[0095] For the existing applications (e.g., social network and/or mobile apps) with binary privacy options (e.g., only binary privacy option), the privacy levels in the template may be mapped to binary value(s). Binary values may include 0 or 5, which may refer to opting in or opting out. For example, a location service may be either on or off (e.g., 0 or 5). At this minimal function level, users may not have control over how raw data, model, and/or score are to be shared with other service providers. The application and/or service providers may have a policy of not sharing any user data, and/or releasing any data, to partners. Users may have no control and/or knowledge if user privacy may have been compromised.

[0096] The user interface template provided may be similar to the browser security setting, which may be easier to use than specifying multiple filtering rules for email filter. For example, once the service provider creates a template for an application with information (e.g., location, time, etc.) and/or other application specific contexts, the menu may generate options for each entry for users to select (e.g., click) and/or to select privacy levels for raw data, model, and/or scores, under different context provided by the template. The user may select (e.g., need to select, such as click) and/or set privacy levels for attribute and/or value pairs (e.g., each attribute and/or value pairs) for the specific contexts that the user may like to have particular privacy levels (e.g., high level privacy protections). The user may leave the rest of the attribute and/or value pairs as default. With the understanding of a trade-off (e.g., to receive the personalized service) defined in the maximal service privacy level requirement, users may adjust the privacy levels above and/or below the maximal level (e.g., may adjust the privacy levels above and/or below the maximal level separately). The default user privacy level settings may be based on maximal personal privacy level requirement(s). The maximal personal privacy level requirement(s) may be defined for applications (e.g., each of the applications) by service providers.

[0097] Users may choose privacy levels for raw data, model, and/or scores (e.g., may choose privacy levels for raw data, model, and/or scores, based on the context). For example, users may choose, because of advantages, to decide privacy levels for raw data, model, and/or scores, separately. A user may set a privacy level (e.g., a high privacy level, medium privacy level, low privacy level) on a model (e.g., a “play time behavior history” model) and/or a score that may identify the user. For example, a user may set a privacy level on a model and/or a score that may identify the user as fanatic player and/or VIP spender, to a third party. The user may set the privacy level when the user is not playing a game. A user may set a model (e.g., history model) to a different privacy level than the privacy level of a score (e.g., classification score). For example, a user may set a model (e.g., play time history model) to a high privacy level while setting a score (e.g., classification score, such as VIP status) to a minimal level. The user may set a model to a high privacy level while setting a score to a minimal level, to receive bonus points and/or VIP treatment to a game developer of the specific game. A user may set high level protection on score (e.g., spending classification score, such as VIP status) and/or allow raw data with medium privacy to be shared. The service provider may provide entries for users to specify how long to keep the raw data, model, and/or score in different time duration. For example, a user may choose to have one or more (e.g., different) score retention periods (e.g., longer, shorter, etc.) than the model and/or the raw data.

[0098] Multiple privacy level settings for models may relate to location based navigation services. The service provider may collect locations (e.g., user locations) and/or predict where the user may be visiting. For example, the service provider may collect locations and/or predict where the user may be visiting based on past history. This location trajectory model may be shared with business partners (e.g., restaurant service, gas station services, etc.) to provide personalized services that may benefit the users. When a user makes purchase transactions and/or is visiting a place (e.g., a hospital), the user may not want to reveal the transaction history and/or raw data to third party service providers. The user may raise the privacy level for the location trajectory model for the specific application to protect privacy.

[0099] Using the GUI interfaces and/or APIs, service providers and/or users may cooperate by sharing the statistical data stored in the metadata repository (e.g., privacy meta data repository 114, as shown in FIG. 1 and FIG. 2). For example, a trajectory model built from various user behavior data collected by multiple service providers in different contexts (e.g., location, time, and/or application) may be combined (e.g., linked) and/or stored in the privacy metadata repository 114. Using the trajectory model, service providers may predict where the user may be likely to visit and/or offer personalized service based on the context. Depending upon the privacy level setting by a user on raw data, model, and/or score, the service provider may share the anonymized location data (e.g., anonymized location data for a user) to other service providers using the metadata repository. For example, the service provider may share the anonymized location data to other service providers using the metadata repository in real-time. Depending upon model and/or score privacy level, the proposed system may provide an anonymous model and/or score to the service providers. For example, the trajectory model may contain purchase records from gas service and/or in combination with restaurant service and/or Uber service that may need to be protected. It may be known that with multiple transaction records in a few (> 4) locations, the identity of the person may be compromised with high probability. A user may use the proposed system to protect privacy and/or authorize specific service provider to access to specific score and/or classification and/or block trajectory model sharing to obtain reward and/or bonus on demand.

[0100] The value added services (e.g., third party value added services) may define templates and/or special functions to provide additional privacy protection services. Value added services may use rules (e.g., dynamically created rules) to access value added privacy protection functions. For example, value added services may use dynamically created rules to access value added privacy protection functions such as on demand score release and/or other advanced features. The advanced feature may include functions to track the life cycle of user data. For example, the advanced feature may include functions to track the life cycle of user data from raw data, model, to score. The advanced feature may track which service providers may have obtained the anonymous data. The advanced feature may provide a function for a user to define which data under what circumstance may be used by one or more specific service provider.

[0101] New System Wide Service Solution and Operation may be described herein. The new system wide service solutions based on the proposed multi-level privacy protection, service action trade-off, and/or data release support functions may be described herein. Based on the service APIs, service providers that offer the applications and/or services may provide the raw data, model, score, and/or service action templates for users to configure and/or update the privacy level settings. The data (e.g., all the data) may be stored (e.g., stored in the metadata repository, such as privacy metadata repository 114). The third party service provider may provide new value added services utilizing the API provided for the privacy metadata repository. The privacy preserving methods and/or systems may be owned and/or operated by a service provider. The server provider may be independent from the application and/or service providers and third party service providers. The independent service providers that may own and/or operate the multi-level privacy protection service may be referred to as MPP service provider (e.g., MPPSP). There may be one or more MPPSPs.

[0102] Service providers of each of the example services may collect, analyze, profile, and/or offer personalized service actions to the users. The service providers may use the API provided by the MPPSPs. As shown in FIG. 1 and FIG. 2, service providers and/or value added services may use the provisioning API to create the service templates. The data sharing function and/or permission among service providers may be managed by the MPPSP. Service providers may configure the business partner lists in the MPPSP, and/or share data with the service partner through the MPPSP. The access control information may be managed by the metadata repository. Business partners may share raw, model, and/or score data with each other using existing data sharing mechanisms. One example sharing mechanism may be to use the access control list for each business partner for each data set.

[0103] One or more (e.g., three) IoT related application and/or service examples may be used to describe the relationships between the service providers, value added services (e.g., third party value added service), users, and/or the service provider (e.g., MPPSP) who operate a multi-level privacy protection service using the proposed methods and/or systems. The three new application services are described herein.

[0104] Wearable Bio-Sign monitoring wearable application service may be a (e.g., a new) application service. The advance in wearable device and/or mobile application may support the personal health and/or bio-sign monitoring applications (e.g., HealthKit, MapMyWalk, etc.). The Bio-sign may be useful for one or more applications (e.g., health care, training, attention level, intensity of exercise, and/or target marketing). The wearable Bio-Sign monitoring wearable application service may register with MPPSP to share one or more types of data (e.g., raw data on the user's current condition, model data to know abnormal condition, and/or score) with business partners to know if the user may have an abnormal condition.

[0105] Road hazard and emergency assistant service may be a (e.g., a new) application service. The road hazard and emergency assistant service may provide service actions (e.g., early warning of road hazard alert, proactive emergency assistance, etc.) for users. For example, through arrangements (e.g., separate arrangements) with business partners, the road hazard and emergency assistant service may obtain privacy protected data from MPPSP directly and/or from the business partner. The road hazard and emergency assistant service may collect road hazard information from IoT sensors (e.g., car sensors for pot hole, traffic congestions, etc.) and Bio-Sign data from the MPPSP. The road hazard and emergency assistant service may collect more accurate location (e.g., within 1 to 10 meters) and sensitive Bio-Sign data. For example, the road hazard and emergency assistant service may use raw data to determine the location of the user and/or personal motion trajectory pattern model and/or score data (e.g., predicting the future location and/or detecting an abnormal behavior). The road hazard and emergency assistant service may use the data from IoT sensors to know the temperature, congestion, and/or other natural disaster that may have occurred and/or is likely to occur in the proximity of the user.

[0106] Mobile app and/or game hosting services may be an application service. The mobile app and/or game hosting service may analyze user behavior data collected from multiple apps and/or games. The mobile app and/or game hosting service provider may partner with IoT network and/or services providers (e.g., Bio-Sign monitoring, Road hazard, and/or emergency assistance service) to provide personalized services under the privacy protection of MPPSP (data sharing through MPPSP). The data that may be shared with the partners may include raw data (e.g., play time and/or achievement log), user behavior pattern model (e.g., play time distribution based on time of the day and/or location for one or more users on one or more games) and/or score (e.g., classification of the users as VIP spender, beginner, and/or other based on preference).

[0107] A value added service may provide advanced privacy protection. For example, a value added service may provide advanced privacy protection based on the API and/or GUI provided by the MPPSP. The value added service may use complex event patterns to detect patterns that may provide indications of privacy leaks and/or violation of anonymity level specified by the users and/or service providers. Using the provisioning interface provided by the MPPSP and/or the additional value added service, service providers (e.g., Bio-sign, Road hazard, emergency assistance, and/or mobile app hosting service providers) may share the data (e.g., share the data with each other). Data sharing may be supported by the various authentication methods and/or by other data sharing methods that may be available. For example, a registry (e.g., a centralized registry) provided by MPPSP may be used to manage and/or reduce the complexity of managing multiple pair-wise sharing policy and/or mechanisms. Service providers may make the templates available. For example, service providers may make the templates available for value added services through the metadata repository.

[0108] The applications and/or value added service providers (SPs) registered to the service may sign and/or conform (e.g., be required to sign and/or conform) to privacy policy agreements with MPPSP. For example, the applications and/or value added service providers (SPs) registered to the service may be required to sign and/or conform to privacy policy agreements with MPPSP to share data with business partners and/or to use (e.g., only use) the privacy protected versions of raw data, models, and/or scores from partners through the MPPSP. After the registration process, the service provider may be authorized to use a MPPSP. The service provider may be authorized to use a MPPSP with a link to the MPPSP introduction and/or sign-on site (e.g., URI). In the high level privacy policy agreement conformation perspective, the MPPSP may be similar to the Web site privacy protection certification service (e.g., existing Web site privacy protection certification service) offered by vendor (e.g., TRUSTe and/or ESRB). These privacy audit service companies may help ensure website privacy practices, meet the applicable regulatory and/or industry standards, and/or provide certificates for websites that pass privacy protection audit. The privacy audit service companies may provide tools to scan third party tracker and/or insights into personally identifiable information data collection.

[0109] MPPSPs may protect privacy of the collected data and/or offer real-time privacy preserving data sharing service for one or more service providers to share raw data, model, and/or scores (e.g., based on context aware multi-level privacy settings). The context aware multiple level privacy setting may be of particular importance. For example, the context aware multiple level privacy setting may be important for IoT enabled applications and/or games where a large number of physical and/or personal information with context information may be collected and/or shared (e.g., collected and/or shared in real-time). If the data is collected (e.g., directly collected) from the IoT device and/or mobile application services, and/or analyzed by the MPPSP, the privacy protection policy may be enforced by the MPPSP (e.g., enforced directly).

[0110] After registering with the MPPSP, administrators of service providers may use API and/or GUI, shown in FIG. 1, to create, configure, and/or update entries in the service action privacy and/or user privacy templates. The service provider may use the value added privacy monitoring and/or violation detection service offered by MPPSP. The service provider may enter business partners in a partner list and/or manage the sharing permission for each type of the data (e.g. for various types of raw data, models, scores, and/or service action data). FIG. 8 shows an example of how a user may go through the Bio-Sign monitoring application services. For example, FIG. 8 shows an example of how a user may go through the Bio-Sign monitoring application services to browse the MPPSP site and/or sign-on to the MPPSP service to manage multiple level privacy on raw data, model, and/or scores.

[0111] The user sign-on and/or privacy control process for the MPPSP may start from a service provider's web page 800 (e.g., Bio-Sign GUI). A privacy statement 802 may define how the data may be collected and/or used by the service provider. The description in the privacy statement 802 may be high level and/or the privacy statement 802 may not provide (e.g. a user may not know before interacting with the MPPSP) specifically and/or exactly how much of the user data is collected, merged with data from other sources (e.g., social network), and/or shared by the SP to business partners. If the service provider is registered and/or the service provider agrees to the privacy policy of MPPSP, the service provider may indicate (e.g., via a website and/or an icon 804 on the website) that the service provider conforms to MPP. By clicking an icon linked to the MPPSP Web services, the user may open the main page of MPP service 806. Clicking an icon linked to the MPPSP Web services to open the main page of MPP service 806 may be similar to clicking a TRUSTe icon to get the description and/or verification information of the service provider.

[0112] The MPP main service page 806 may contain a list of features describing the benefits of MPP that may be offered and/or used by the service provider. Bio-Sign service provider may use predictive analytic tools provided by MPPSP to derive statistical distribution models (e.g., average, standard deviation, and/or clustering models). The model data may contain pulse, exercise, and/or sleep patterns. The user may realize that this data may reveal sensitive personal information and/or the user's identity. Based on users' privacy concern on the raw data, summary behavior pattern model, and/or the abnormality classification, the user may set different privacy levels for different service providers. When the user has a question (e.g., a question about the meaning of anonymity), "help" information 812, 814 may be provided. For example, "help" information 812, 814 may be provided for the user to browse and/or understand the mapping between privacy level and the effect of a privacy level setting. Mapping between privacy level and the effect of a privacy level setting may include the number of anonymous users to be included in a subset of shared data. The subset of shared data may include users of an equivalent class with the same or similar quasi-identifiers, such as time, location device type, age, monthly spending, and/or play time.

[0113] Users may use the GUI 806 provided by MPPSP, as shown in FIG .8, for the service feature offered by Bio-Sign application service provider (e.g., SP1). For example, SP1 may offer one or more of the following Multi-level privacy protection (MPP) features through the MPPSP.

[0114] A feature offered by a service provider may include Bio-Sign history (e.g., Bio-Sign history used by SP1). The Bio-Sign history may not be released to other business partners. For example, the Bio-Sign history may not be released to other business partners without having the user's permission. Users may be able to obtain a list of partners. For example, users may be able to obtain a list of partners by referring to a partner list (e.g., Bio-Sign service partner list) after singing on and/or logging on to MPPSP.

[0115] A feature offered by a service provider may include the behavior pattern (e.g., average pulse rate distribution over the time of day) being set with anonymity level of 100. The service provider may include the behavior pattern set with an anonymity level of 100 when the data is released to business partners. Including the behavior pattern set with an anonymity level of 100 may provide good protection for privacy. For example, including the behavior pattern set with an anonymity level of 100 may provide good protection for privacy because the service provider may not distinguish one user from other users (e.g., the other 99 users) using the other personal data (e.g., quasi-identifiers) released with the data.

[0116] A feature offered by a service provider may include persons with physical irregularities (e.g., abnormal pulse and/or sweat patterns) being kept confidential. For example, the service provider may keep the degree of irregularity scores in the top or bottom percentile confidential. The confidential information may be released upon user's request.

[0117] A feature offered by a service provider may include bio-sign data collected with location tracking service having high anonymity (e.g., 1000).

[0118] A feature offered by a service provider may include a user adjusting the privacy setting of Bio-Sign and/or location predicative behavior pattern model. For example, a feature offered by a service provider may include a user adjusting the privacy setting of Bio-Sign and/or location predicative behavior pattern model based on a service action privacy level (e.g., maximum service action privacy level) defined by service applications and/or actions on-demand (e.g., road hazard, emergency assistance, nearest gas station, and/or treadmill services) to receive just-in-time personalized service (e.g., early warning of medical conditions and/or notification for VIP reservation).

[0119] After reading the benefits of the MPPSP, the user may sign-on 808 to the MPPSP. After sign-on, the user may add the application (e.g., Bio-Sign) 810 to the user account. User may add one or more application services (e.g., road hazard service, games, IoT Apps, such as Treadmill, and/or a Bio-Sign monitoring service. The list of application services may be displayed (e.g., displayed in a menu) for the user to configure and/or update the privacy level for a new and/or existing activities.

[0120] As shown in FIG. 8, when the user selects (e.g., clicks) a registered service (e.g., Bio-Sign service 816), the user may access the user privacy setting examples 818 and/or the service action privacy setting examples 820related to the Bio-Sign service. The user privacy setting examples 818 and/or the service action privacy setting examples 820 may be one or more user privacy setting templates and/or one or more service action privacy setting templates. Business partners for the service provider may be listed. For example, business partners for the service provider may be listed so the user knows the relationships and/or consequences of revealing data (e.g., revealing data to the business partners). For example, the service action privacy template 820 may specify the privacy requirements rules for different service actions (e.g., privacy level of Pulse raw data, PL(Pulse) ≤ 3 for Road hazard and/or emergency assistance service, privacy level of location predictive model, PL(Location).model ≤ 3 for road hazard service, privacy level setting for Pulse and/or temperature score against the distribution model, PL(Pulse|Temp).score ≤ 5 for road hazard and/or emergency assistance.)

[0121] A user may change the privacy level setting for raw data, behavior model, and/or scores in the multi-level privacy protection configuration template. For example, a user may change the privacy level setting for raw data, behavior model, and/or scores in the multi-level privacy protection configuration template based on a maximal privacy level setting for service actions using the GUI templates. For example, a user may block (e.g., completely block) the data sharing (e.g., the data sharing to advertising network) by setting the privacy level (e.g., privacy level to advertising network service) to “5” for the raw data. The user may provide feedback on a privacy concern rating on the statistical behavior model. For example, the user may provide feedback on a privacy concern rating on the statistical behavior model if the user receives advertisement of direct marking email on a topic related to the behavior model.

[0122] Recognizing that privacy protection issues may be complex (e.g., privacy protection issues may be as complex as that of data security protection), the multiple value-added service features may be provided by the MPPSP and/or third party service providers. Based on the unified data model managed by the metadata repository, multiple privacy protection service features may share the data model 822 and/or be integrated in one unified GUI interface. Multiple value added services may be provided (e.g., provided seamlessly) to the user. For example, multiple value added services may be provided to the user using a unified GUI with one or more overlays. The anonymity level of the data set (e.g., raw data, behavior model data, score data, and/or ranking and/or categorization of the data against the behavior model) may be listed together. For example, the anonymity level of the data set may be listed together with recommended settings from the value added service providers.

[0123] The value added services may display relationships (e.g., high level relationships) between service providers. As shown in FIG. 9, one or more (e.g., each) relationships may be modeled as a link with summary privacy level setting and/or anonymity count statistics collected from a large number of users. For example, relationships pulse 902, temperature 904, sweat 906, and location 908 may be modeled as a link with summary privacy level setting and/or anonymity count statistics collected from a large number of users. The statistics may help the user to understand that the anonymity level of the data is being shared. For example, the statistics may help the user to understand that the anonymity level of the data is being shared between the service providers and/or their partners. The statistics may contain information about how users (e.g., other users) set the privacy level setting and/or the feedback on the service actions provided by service providers. With the statistical information, users may decide how to set the privacy level. For example, with this statistical information, users may decide how to set the privacy level based on settings (e.g., commonly used settings, such as average, settings) for the application services.

[0124] A user may drill down to a link representing the relationships between a service provider and/or a business partner. For example, a user may drill down to a link representing the relationships between a service provider and/or a business partner who may offer additional service actions to the user. To aid the user in this task, one or more of the following informational reference settings may be provided. For example, a maximum setting 910 (e.g., a setting required by the service action provider to provide a service, such as road hazard service) may be provided. An average privacy setting 912 of other users (e.g., an average privacy setting of other users with similar behavior patterns) may be provided, and/or a recommended privacy setting 914 may be provided. As shown in "1" of FIG. 9, a user may select (e.g., click) and/or check the privacy setting on how the Bio-Sign service 914 may protect the user privacy. For example, a user may select and/or check the privacy setting on how the Bio-Sign service 914 may protect the user privacy when sharing the data with a partner (e.g., Road hazard and emergency assistance service 916). A user may click on an entry (e.g., a specific entry, such as the score privacy level for Pulse data) in the privacy setting template 920 to activate a separate GUI 922. The separate GUI 922 may have a help menu (e.g., to explain the meaning of the privacy settings, such as Max 910, Avg 912, Recommended 914). Based on the explanations, a user may decide to add and/or change the privacy setting to a preferred level (e.g., 3).

[0125] The user may select (e.g., click) and/or see the number of services that were blocked. For example, the user may select and/or see the number of services that were blocked because the privacy level setting used by the user is set differently (e.g., higher, lower, etc.) than the maximal privacy level allowed by the service action. For example, the Bio-Sign score may be released (e.g., released on demand) to provide accurate location and/or the abnormal condition with raw data for urgent medical assistance.

[0126] The recommended 914 privacy setting may be provided by a value added privacy setting recommendation service. The privacy recommendation service may provide a level of user profiling to divide the users into groups. The groups may be based on business related criteria, such as health and/or safety (e.g., Bio-Sign, Road hazard, and/or emergency assistance services) to help users configure the privacy level setting. The recommendation service may use personalized preference information obtained from the user. For example, the recommendation service may use personalized preference information obtained from the user to set the privacy levels (e.g., set the privacy levels automatically) and/or change the level to support on-demand privacy adjustment for personalized service actions. For example, the recommendation service may help a user to set the privacy level setting based on average setting of user with similar behavior patterns (e.g., abnormal pulse). As shown in FIG. 9, the recommended privacy level setting for raw data may be adjusted (e.g., adjusted lower) to ensure that the user may be identified more accurately. The recommended privacy setting may raise the privacy level for the trajectory pattern (e.g., spatial and/or temporal model) that may have included the statistics of the places (e.g., all the places) the user had visited for a time period (e.g., the past three months). To allow for identification of real time abnormal behavior patterns, the privacy level for score data may be lowered. For example, to allow for identification of real time abnormal behavior patterns, the privacy level for score data may be lowered so that the user can be located accurately for emergency service.

[0127] The privacy setting recommendation service may use a health condition as criteria to categorize the user into groups. The recommendation service may use one or more (e.g., one or more other) conditions and/or preference information associated with food, clothing, home, transportation, social, and/or entertainment for other service partners in the corresponding business areas. Various existing clustering methods may be used to obtain numbers (e.g., small numbers, large numbers, etc.) of user groups for business areas. Users may be grouped based on one or more topics. For business areas, the privacy setting recommendation system may calculate the privacy setting distribution and/or recommend a suitable (e.g., average) privacy level for the user. The service may report the anonymity counts and/or quasi-identifiers associated with the anonymity counts for raw data, model, and/or score used by the service providers or by the MPPSP.

[0128] A value added service feature may collect feedback from the user on a privacy concern rating. The value added service feature may update the service action privacy concern rating (e.g., collect and/or update the service action privacy concern rating automatically). For example, a user may receive a call (e.g., an advertisement and/or a marketing call) that is related to a recent activity (e.g., special type of medical assistance and/or special place visited). As a result of the call, if the user feels that privacy was violated (e.g., potentially violated), the user may provide feedback to the value added privacy concern feedback service provider. The feedback management service may be invoked by clicking on a MPP feedback icon with the advertisement.

[0129] FIG. 10A is a diagram of an example communications system 1000 in which one or more disclosed embodiments may be implemented. The communications system 1000 may be a multiple access system that provides content, such as voice, data, video, messaging, broadcast, *etc.*, to multiple wireless users. The communications system 1000 may enable multiple wireless users to access such content through the sharing of system resources, including wireless bandwidth. For example, the communications systems 1000 may employ one or more channel access methods, such as code division multiple access (CDMA), time division multiple access (TDMA), frequency division multiple access (FDMA), orthogonal FDMA (OFDMA), single-carrier FDMA (SC-FDMA), and the like.

[0130] As shown in FIG. 10A, the communications system 1000 may include wireless transmit/receive units (WTRUs) 1002a, 1002b, 1002c, and/or 1002d (which generally or collectively may be referred to as WTRU 1002), a radio access network (RAN) 1003/1004/1005, a core network 1006/1007/1009, a public switched telephone network (PSTN) 1008, the Internet 1010, and other networks 1012, though it will be appreciated that the disclosed embodiments contemplate any number of WTRUs, base stations, networks, and/or network elements. Each of the WTRUs 1002a, 1002b, 1002c, 1002d may be any type of device configured to operate and/or communicate in a wireless environment. By way of example, the WTRUs 1002a, 1002b, 1002c, 1002d may be configured to transmit and/or receive wireless signals and may include user equipment (UE), a mobile station, a fixed or mobile subscriber unit, a pager, a cellular telephone, a personal digital assistant (PDA), a smartphone, a laptop, a netbook, a personal computer, a wireless sensor, consumer electronics, and the like.

[0131] The communications systems 1000 may also include a base station 1014a and a base station 1014b. Each of the base stations 1014a, 1014b may be any type of device configured to wirelessly interface with at least one of the WTRUs 1002a, 1002b, 1002c, 1002d to facilitate access to one or more communication networks, such as the core network 1006/1007/1009, the Internet 1010, and/or the networks 1012. By way of example, the base stations 1014a, 1014b may be a base transceiver station (BTS), a Node-B, an eNode B, a Home Node B, a Home eNode B, a site controller, an access point (AP), a wireless router, and the like. While the base stations 1014a, 1014b are each depicted as a single element, it will be appreciated that the base stations 1014a, 1014b may include any number of interconnected base stations and/or network elements.

[0132] The base station 1014a may be part of the RAN 1003/1004/1005, which may also include other base stations and/or network elements (not shown), such as a base station controller (BSC), a radio network controller (RNC), relay nodes, *etc.* The base station 1014a and/or the base station 1014b may be configured to transmit and/or receive wireless signals within a particular geographic region, which may be referred to as a cell (not shown). The cell may further be divided into cell sectors. For example, the cell associated with the base station 1014a may be divided into three sectors. Thus, in one embodiment, the base station 1014a may include three transceivers, *e.g.*, one for each sector of the cell. In another embodiment, the base station 1014a may employ multiple-input multiple output (MIMO) technology and, therefore, may utilize multiple transceivers for each sector of the cell.

[0133] The base stations 1014a, 1014b may communicate with one or more of the WTRUs 1002a, 1002b, 1002c, 1002d over an air interface 1015/1016/1017, which may be any suitable wireless communication link (*e.g.*, radio frequency (RF), microwave, infrared (IR), ultraviolet (UV), visible light, *etc.*). The air interface 1015/1016/1017 may be established using any suitable radio access technology (RAT).

[0134] More specifically, as noted above, the communications system 1000 may be a multiple access system and may employ one or more channel access schemes, such as CDMA, TDMA, FDMA, OFDMA, SC-FDMA, and the like. For example, the base station 1014a in the RAN 1003/1004/1005 and the WTRUs 1002a, 1002b, 1002c may implement a radio technology such as Universal Mobile Telecommunications System (UMTS) Terrestrial Radio Access (UTRA), which may establish the air interface 1015/1016/1017 using wideband CDMA (WCDMA). WCDMA may include communication protocols such as High-Speed Packet Access (HSPA) and/or Evolved HSPA (HSPA+). HSPA may include High-Speed Downlink Packet Access (HSDPA) and/or High-Speed Uplink Packet Access (HSUPA).

[0135] In another embodiment, the base station 1014a and the WTRUs 1002a, 1002b, 1002c may implement a radio technology such as Evolved UMTS Terrestrial Radio Access (E-UTRA), which may establish the air interface 1015/1016/1017 using Long Term Evolution (LTE) and/or LTE-Advanced (LTE-A).

[0136] In other embodiments, the base station 1014a and the WTRUs 1002a, 1002b, 1002c may implement radio technologies such as IEEE 802.16 (*e.g.*, Worldwide Interoperability for Microwave Access (WiMAX)), CDMA2000, CDMA2000 1X, CDMA2000 EV-DO, Interim Standard 2000 (IS-2000), Interim Standard 95 (IS-95), Interim Standard 856 (IS-856), Global System for Mobile communications (GSM), Enhanced Data rates for GSM Evolution (EDGE), GSM EDGE (GERAN), and the like.

[0137] The base station 1014b in FIG. 10A may be a wireless router, Home Node B, Home eNode B, or access point, for example, and may utilize any suitable RAT for facilitating wireless connectivity in a localized area, such as a place of business, a home, a vehicle, a campus, and the like. In one embodiment, the base station 1014b and the WTRUs 1002c, 1002d may implement a radio technology such as IEEE 802.11 to establish a wireless local area network (WLAN). In another embodiment, the base station 1014b and the WTRUs 1002c, 1002d may implement a radio technology such as IEEE 802.15 to establish a wireless personal area network (WPAN). In yet another embodiment, the base station 1014b and the WTRUs 1002c, 1002d may utilize a cellular-based RAT (*e.g.*, WCDMA, CDMA2000, GSM, LTE, LTE-A, *etc.*) to establish a picocell or femtocell. As shown in FIG. 10A, the base station 1014b may have a direct connection to the Internet 1010. Thus, the base station 1014b may not be required to access the Internet 1010 via the core network 1006/1007/1009.

[0138] The RAN 1003/1004/1005 may be in communication with the core network 1006/1007/1009, which may be any type of network configured to provide voice, data, applications, and/or voice over internet protocol (VoIP) services to one or more of the WTRUs 1002a, 1002b, 1002c, 1002d. For example, the core network 1006/1007/1009 may provide call control, billing services, mobile location-based services, pre-paid calling, Internet connectivity, video distribution, *etc.*, and/or perform high-level security functions, such as user authentication. Although not shown in FIG. 10A, it will be appreciated that the RAN 1003/1004/1005 and/or the core network 1006/1007/1009 may be in direct or indirect communication with other RANs that employ the same RAT as the RAN 1003/1004/1005 or a different RAT. For example, in addition to being connected to the RAN 1003/1004/1005, which may be utilizing an E-UTRA radio technology, the core network 1006/1007/1009 may also be in communication with another RAN (not shown) employing a GSM radio technology.

[0139] The core network 1006/1007/1009 may also serve as a gateway for the WTRUs 1002a, 1002b, 1002c, 1002d to access the PSTN 1008, the Internet 1010, and/or other networks 1012. The PSTN 1008 may include circuit-switched telephone networks that provide plain old telephone service (POTS). The Internet 1010 may include a global system of interconnected computer networks and devices that use common communication protocols, such as the transmission control protocol (TCP), user datagram protocol (UDP) and the internet protocol (IP) in the TCP/IP internet protocol suite. The networks 1012 may include wired or wireless communications networks owned and/or operated by other service providers. For example, the networks 1012 may include another core network connected to one or more RANs, which may employ the same RAT as the RAN 1003/1004/1005 or a different RAT.

[0140] Some or all of the WTRUs 1002a, 1002b, 1002c, 1002d in the communications system 1000 may include multi-mode capabilities, *e.g.*, the WTRUs 1002a, 1002b, 1002c, 1002d may include multiple transceivers for communicating with different wireless networks over different wireless links. For example, the WTRU 1002c shown in FIG. 10A may be configured to communicate with the base station 1014a, which may employ a cellular-based radio technology, and with the base station 1014b, which may employ an IEEE 802 radio technology.

[0141] FIG. 10B is a system diagram of an example WTRU 1002. As shown in FIG. 10B, the WTRU 1002 may include a processor 1018, a transceiver 1020, a transmit/receive element 1022, a speaker/microphone 1024, a keypad 1026, a display/touchpad 1028, non-removable memory 1030, removable memory 1032, a power source 1034, a global positioning system (GPS) chipset 1036, and other peripherals 1038. It will be appreciated that the WTRU 1002 may include any sub-combination of the foregoing elements while remaining consistent with an embodiment. Also, embodiments contemplate that the base stations 1014a and 1014b, and/or the nodes that base stations 1014a and 1014b may represent, such as but not limited to transceiver station (BTS), a Node-B, a site controller, an access point (AP), a home node-B, an evolved home node-B (eNodeB), a home evolved node-B (HeNB), a home evolved node-B gateway, and proxy nodes, among others, may include some or all of the elements depicted in FIG. 10B and described herein.

[0142] The processor 1018 may be a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Array (FPGAs) circuits, any other type of integrated circuit (IC), a state machine, and the like. The processor 1018 may perform signal coding, data processing, power control, input/output processing, and/or any other functionality that enables the WTRU 1002 to operate in a wireless environment. The processor 1018 may be coupled to the transceiver 1020, which may be coupled to the transmit/receive element 1022. While FIG. 10B depicts the processor 1018 and the transceiver 1020 as separate components, it will be appreciated that the processor 1018 and the transceiver 1020 may be integrated together in an electronic package or chip.

[0143] The transmit/receive element 1022 may be configured to transmit signals to, or receive signals from, a base station (*e.g.*, the base station 1014a) over the air interface 1015/1016/1017. For example, in one embodiment, the transmit/receive element 1022 may be an antenna configured to transmit and/or receive RF signals. In another embodiment, the transmit/receive element 1022 may be an emitter/detector configured to transmit and/or receive

IR, UV, or visible light signals, for example. In yet another embodiment, the transmit/receive element 1022 may be configured to transmit and receive both RF and light signals. It will be appreciated that the transmit/receive element 1022 may be configured to transmit and/or receive any combination of wireless signals.

[0144] In addition, although the transmit/receive element 1022 is depicted in FIG. 10B as a single element, the WTRU 1002 may include any number of transmit/receive elements 1022. More specifically, the WTRU 1002 may employ MIMO technology. Thus, in one embodiment, the WTRU 1002 may include two or more transmit/receive elements 1022 (*e.g.*, multiple antennas) for transmitting and receiving wireless signals over the air interface 1015/1016/1017.

[0145] The transceiver 1020 may be configured to modulate the signals that are to be transmitted by the transmit/receive element 1022 and to demodulate the signals that are received by the transmit/receive element 1022. As noted above, the WTRU 1002 may have multi-mode capabilities. Thus, the transceiver 1020 may include multiple transceivers for enabling the WTRU 1002 to communicate via multiple RATs, such as UTRA and IEEE 802.11, for example.

[0146] The processor 1018 of the WTRU 1002 may be coupled to, and may receive user input data from, the speaker/microphone 1024, the keypad 1026, and/or the display/touchpad 1028 (*e.g.*, a liquid crystal display (LCD) display unit or organic light-emitting diode (OLED) display unit). The processor 1018 may also output user data to the speaker/microphone 1024, the keypad 1026, and/or the display/touchpad 1028. In addition, the processor 1018 may access information from, and store data in, any type of suitable memory, such as the non-removable memory 1030 and/or the removable memory 1032. The non-removable memory 1030 may include random-access memory (RAM), read-only memory (ROM), a hard disk, or any other type of memory storage device. The removable memory 1032 may include a subscriber identity module (SIM) card, a memory stick, a secure digital (SD) memory card, and the like. In other embodiments, the processor 1018 may access information from, and store data in, memory that is not physically located on the WTRU 1002, such as on a server or a home computer (not shown).

[0147] The processor 1018 may receive power from the power source 1034, and may be configured to distribute and/or control the power to the other components in the WTRU 1002. The power source 1034 may be any suitable device for powering the WTRU 1002. For example, the power source 1034 may include one or more dry cell batteries (*e.g.*, nickel-cadmium (NiCd), nickel-zinc (NiZn), nickel metal hydride (NiMH), lithium-ion (Li-ion), *etc.*), solar cells, fuel cells, and the like.

[0148] The processor 1018 may also be coupled to the GPS chipset 1036, which may be configured to provide location information (*e.g.*, longitude and latitude) regarding the current location of the WTRU 1002. In addition to, or in lieu of, the information from the GPS chipset 1036, the WTRU 1002 may receive location information over the air interface 1015/1016/1017 from a base station (*e.g.*, base stations 1014a, 1014b) and/or determine its location based on the timing of the signals being received from two or more nearby base stations. It will be appreciated that the WTRU 1002 may acquire location information by way of any suitable location-determination method while remaining consistent with an embodiment.

[0149] The processor 1018 may further be coupled to other peripherals 1038, which may include one or more software and/or hardware modules that provide additional features, functionality and/or wired or wireless connectivity. For example, the peripherals 1038 may include an accelerometer, an e-compass, a satellite transceiver, a digital camera (for photographs or video), a universal serial bus (USB) port, a vibration device, a television transceiver, a hands free headset, a Bluetooth® module, a frequency modulated (FM) radio unit, a digital music player, a media player, a video game player module, an Internet browser, and the like.

[0150] FIG. 10C is a system diagram of the RAN 1003 and the core network 1006 according to an embodiment. As noted above, the RAN 1003 may employ a UTRA radio technology to communicate with the WTRUs 1002a, 1002b, 1002c over the air interface 1015. The RAN 1003 may also be in communication with the core network 1006. As shown in FIG. 10C, the RAN 1003 may include Node-Bs 1040a, 1040b, 1040c, which may each include one or more transceivers for communicating with the WTRUs 1002a, 1002b, 1002c over the air interface 1015. The Node-Bs 1040a, 1040b, 1040c may each be associated with a particular cell (not shown) within the RAN 1003. The RAN 1003 may also include RNCs 1042a, 1042b. It will be appreciated that the RAN 1003 may include any number of Node-Bs and RNCs while remaining consistent with an embodiment.

[0151] As shown in FIG. 10C, the Node-Bs 1040a, 1040b may be in communication with the RNC 1042a. Additionally, the Node-B 1040c may be in communication with the RNC142b. The Node-Bs 1040a, 1040b, 1040c may communicate with the respective RNCs 1042a, 1042b via an Iub interface. The RNCs 1042a, 1042b may be in communication with one another via an Iur interface. Each of the RNCs 1042a, 1042b may be configured to control the respective Node-Bs 1040a, 1040b, 1040c to which it is connected. In addition, each of the RNCs 1042a, 1042b may be configured to carry out or support other functionality, such as outer loop power control, load control, admission control, packet scheduling, handover control, macrodiversity, security functions, data encryption, and the like.

[0152] The core network 1006 shown in FIG. 10C may include a media gateway (MGW) 1044, a mobile switching center (MSC) 1046, a serving GPRS support node (SGSN) 1048, and/or a gateway GPRS support node (GGSN) 1050. While each of the foregoing elements are depicted as part of the core network 1006, it will be appreciated that any one of these elements may be owned and/or operated by an entity other than the core network operator.

[0153] The RNC 1042a in the RAN 1003 may be connected to the MSC 1046 in the core network 1006 via an IuCS interface. The MSC 1046 may be connected to the MGW 1044. The MSC 1046 and the MGW 1044 may provide the WTRUs 1002a, 1002b, 1002c with access to circuit-switched networks, such as the PSTN 1008, to facilitate communications between the WTRUs 1002a, 1002b, 1002c and traditional land-line communications devices.

[0154] The RNC 1042a in the RAN 1003 may also be connected to the SGSN 1048 in the core network 1006 via an IuPS interface. The SGSN 1048 may be connected to the GGSN 1050. The SGSN 1048 and the GGSN 1050 may provide the WTRUs 1002a, 1002b, 1002c with access to packet-switched networks, such as the Internet 1010, to facilitate communications between and the WTRUs 1002a, 1002b, 1002c and IP-enabled devices.

[0155] As noted above, the core network 1006 may also be connected to the networks 1012, which may include other wired or wireless networks that are owned and/or operated by other service providers.

[0156] FIG. 10D is a system diagram of the RAN 1004 and the core network 1007 according to an embodiment. As noted above, the RAN 1004 may employ an E-UTRA radio technology to communicate with the WTRUs 1002a, 1002b, 1002c over the air interface 1016. The RAN 1004 may also be in communication with the core network 1007.

[0157] The RAN 1004 may include eNode-Bs 1060a, 1060b, 1060c, though it will be appreciated that the RAN 1004 may include any number of eNode-Bs while remaining consistent with an embodiment. The eNode-Bs 1060a, 1060b, 1060c may each include one or more transceivers for communicating with the WTRUs 1002a, 1002b, 1002c over the air interface 1016. In one embodiment, the eNode-Bs 1060a, 1060b, 1060c may implement MIMO technology. Thus, the eNode-B 1060a, for example, may use multiple antennas to transmit wireless signals to, and receive wireless signals from, the WTRU 1002a.

[0158] Each of the eNode-Bs 1060a, 1060b, 1060c may be associated with a particular cell (not shown) and may be configured to handle radio resource management decisions, handover decisions, scheduling of users in the uplink and/or downlink, and the like. As shown in FIG. 10D, the eNode-Bs 1060a, 1060b, 1060c may communicate with one another over an X2 interface.

[0159] The core network 1007 shown in FIG. 10D may include a mobility management gateway (MME) 1062, a serving gateway 1064, and a packet data network (PDN) gateway 1066.

While each of the foregoing elements are depicted as part of the core network 1007, it will be appreciated that any one of these elements may be owned and/or operated by an entity other than the core network operator.

[0160] The MME 1062 may be connected to each of the eNode-Bs 1060a, 1060b, 1060c in the RAN 1004 via an S1 interface and may serve as a control node. For example, the MME 1062 may be responsible for authenticating users of the WTRUs 1002a, 1002b, 1002c, bearer activation/deactivation, selecting a particular serving gateway during an initial attach of the WTRUs 1002a, 1002b, 1002c, and the like. The MME 1062 may also provide a control plane function for switching between the RAN 1004 and other RANs (not shown) that employ other radio technologies, such as GSM or WCDMA.

[0161] The serving gateway 1064 may be connected to each of the eNode-Bs 1060a, 1060b, 1060c in the RAN 1004 via the S1 interface. The serving gateway 1064 may generally route and forward user data packets to/from the WTRUs 1002a, 1002b, 1002c. The serving gateway 1064 may also perform other functions, such as anchoring user planes during inter-eNode B handovers, triggering paging when downlink data is available for the WTRUs 1002a, 1002b, 1002c, managing and storing contexts of the WTRUs 1002a, 1002b, 1002c, and the like.

[0162] The serving gateway 1064 may also be connected to the PDN gateway 1066, which may provide the WTRUs 1002a, 1002b, 1002c with access to packet-switched networks, such as the Internet 1010, to facilitate communications between the WTRUs 1002a, 1002b, 1002c and IP-enabled devices.

[0163] The core network 1007 may facilitate communications with other networks. For example, the core network 1007 may provide the WTRUs 1002a, 1002b, 1002c with access to circuit-switched networks, such as the PSTN 1008, to facilitate communications between the WTRUs 1002a, 1002b, 1002c and traditional land-line communications devices. For example, the core network 1007 may include, or may communicate with, an IP gateway (*e.g.*, an IP multimedia subsystem (IMS) server) that serves as an interface between the core network 1007 and the PSTN 1008. In addition, the core network 1007 may provide the WTRUs 1002a, 1002b, 1002c with access to the networks 1012, which may include other wired or wireless networks that are owned and/or operated by other service providers.

[0164] FIG. 10E is a system diagram of the RAN 1005 and the core network 1009 according to an embodiment. The RAN 1005 may be an access service network (ASN) that employs IEEE 802.16 radio technology to communicate with the WTRUs 1002a, 1002b, 1002c over the air interface 1017. As will be further discussed below, the communication links between the different functional entities of the WTRUs 1002a, 1002b, 1002c, the RAN 1005, and the core network 1009 may be defined as reference points.

[0165] As shown in FIG. 10E, the RAN 1005 may include base stations 1080a, 1080b, 1080c, and an ASN gateway 1082, though it will be appreciated that the RAN 1005 may include any number of base stations and ASN gateways while remaining consistent with an embodiment. The base stations 1080a, 1080b, 1080c may each be associated with a particular cell (not shown) in the RAN 1005 and may each include one or more transceivers for communicating with the WTRUs 1002a, 1002b, 1002c over the air interface 1017. In one embodiment, the base stations 1080a, 1080b, 1080c may implement MIMO technology. Thus, the base station 1080a, for example, may use multiple antennas to transmit wireless signals to, and receive wireless signals from, the WTRU 1002a. The base stations 1080a, 1080b, 1080c may also provide mobility management functions, such as handoff triggering, tunnel establishment, radio resource management, traffic classification, quality of service (QoS) policy enforcement, and the like. The ASN gateway 1082 may serve as a traffic aggregation point and may be responsible for paging, caching of subscriber profiles, routing to the core network 1009, and the like.

[0166] The air interface 1017 between the WTRUs 1002a, 1002b, 1002c and the RAN 1005 may be defined as an R1 reference point that implements the IEEE 802.16 specification. In addition, each of the WTRUs 1002a, 1002b, 1002c may establish a logical interface (not shown) with the core network 1009. The logical interface between the WTRUs 1002a, 1002b, 1002c and the core network 1009 may be defined as an R2 reference point, which may be used for authentication, authorization, IP host configuration management, and/or mobility management.

[0167] The communication link between each of the base stations 1080a, 1080b, 1080c may be defined as an R8 reference point that includes protocols for facilitating WTRU handovers and the transfer of data between base stations. The communication link between the base stations 1080a, 1080b, 1080c and the ASN gateway 1082 may be defined as an R6 reference point. The R6 reference point may include protocols for facilitating mobility management based on mobility events associated with each of the WTRUs 1002a, 1002b, 1002c.

[0168] As shown in FIG. 10E, the RAN 1005 may be connected to the core network 1009. The communication link between the RAN 1005 and the core network 1009 may defined as an R3 reference point that includes protocols for facilitating data transfer and mobility management capabilities, for example. The core network 1009 may include a mobile IP home agent (MIP-HA) 1084, an authentication, authorization, accounting (AAA) server 1086, and a gateway 1088. While each of the foregoing elements are depicted as part of the core network

1009, it will be appreciated that any one of these elements may be owned and/or operated by an entity other than the core network operator.

[0169] The MIP-HA may be responsible for IP address management, and may enable the WTRUs 1002a, 1002b, 1002c to roam between different ASNs and/or different core networks. The MIP-HA 1084 may provide the WTRUs 1002a, 1002b, 1002c with access to packet-switched networks, such as the Internet 1010, to facilitate communications between the WTRUs 1002a, 1002b, 1002c and IP-enabled devices. The AAA server 1086 may be responsible for user authentication and for supporting user services. The gateway 1088 may facilitate interworking with other networks. For example, the gateway 1088 may provide the WTRUs 1002a, 1002b, 1002c with access to circuit-switched networks, such as the PSTN 1008, to facilitate communications between the WTRUs 1002a, 1002b, 1002c and traditional land-line communications devices. In addition, the gateway 1088 may provide the WTRUs 1002a, 1002b, 1002c with access to the networks 1012, which may include other wired or wireless networks that are owned and/or operated by other service providers.

[0170] Although not shown in FIG. 10E, it will be appreciated that the RAN 1005 may be connected to other ASNs and the core network 1009 may be connected to other core networks. The communication link between the RAN 1005 the other ASNs may be defined as an R4 reference point, which may include protocols for coordinating the mobility of the WTRUs 1002a, 1002b, 1002c between the RAN 1005 and the other ASNs. The communication link between the core network 1009 and the other core networks may be defined as an R5 reference, which may include protocols for facilitating interworking between home core networks and visited core networks.

[0171] Although features and elements are described above in particular combinations, one of ordinary skill in the art will appreciate that each feature or element may be used alone or in any combination with the other features and elements. Other than the 802.11 protocols described herein, the features and elements described herein may be applicable to other wireless systems. In addition, the methods described herein may be implemented in a computer program, software, or firmware incorporated in a computer-readable medium for execution by a computer or processor. Examples of computer-readable media include electronic signals (transmitted over wired or wireless connections) and computer-readable storage media. Examples of computer-readable storage media include, but are not limited to, a read only memory (ROM), a random access memory (RAM), a register, cache memory, semiconductor memory devices, magnetic media such as internal hard disks and removable disks, magneto-optical media, optical media such as CD-ROM disks, and digital versatile disks (DVDs). A processor in association with software may be used to implement a radio frequency transceiver for use in a WTRU, WTRU, terminal, base station, RNC, or any host computer.

CLAIMS

What Is Claimed:

1. A device for managing multi-level privacy protection, comprising:

    a processor configured to:

    receive a first template relating to a first service provider and a second template relating to a second service provider, wherein the first template comprises a first privacy level and a second privacy level, and wherein the second template comprises a third privacy level and a fourth privacy level, and wherein respective privacy levels are associated with respective levels of privacy to maintain for user information;

    determine, for the respective privacy levels, a respective service that is available or a respective service that is not available, wherein the determination is based on an associated template from an associated service provider;

    provide an indication of the respective service that is available or the respective service that is not available for the respective privacy levels;

    receive an indication of a respective privacy level to use for a respective service provider; and

    coordinate a user interaction with the respective service provider and maintain the indicated respective privacy level associated with the respective service provider.

2. The device of claim 1, wherein the user information is associated with an activity or a location relating to a user.

3. The device of claim 1, wherein the processor is further configured to:

    determine, based on the respective privacy levels, an anonymization level at which the user information is to be anonymized;

    anonymize the user information according to the determined anonymized level; and

    provide the anonymized user information to the first service provider and the second service provider.

4. The device of claim 3, wherein the user information is anonymized via a k-anonymity or a t-closeness process.

5. The device of claim 1, wherein the processor is further configured to:

determine a maximum privacy level for the respective privacy levels, wherein the maximum privacy level corresponds to an accuracy of the user information.

6. The device of claim 5, wherein an effectiveness of the services to be included by the first service provider and the second service provider is based on the accuracy of the user information.

7. The device of claim 1, wherein the indication of the respective privacy level to use for the respective service provider is received via a high level user interface.

8. A method for managing multi-level privacy protection, comprising:

receiving a first template relating to a first service provider and a second template relating to a second service provider, wherein the first template comprises a first privacy level and a second privacy level, and wherein the second template comprises a third privacy level and a fourth privacy level, and wherein respective privacy levels are associated with respective levels of privacy to maintain for user information;

determining, for the respective privacy levels, a respective service that is available or a respective service that is not available, wherein the determination is based on an associated template from an associated service provider;

providing an indication of the respective service that is available or the respective service that is not available for the respective privacy levels;

receiving an indication of a respective privacy level to use for a respective service provider; and

coordinating a user interaction with the respective service provider and maintain the indicated respective privacy level associated with the respective service provider.

9. The method of claim 8, wherein the user information is associated with an activity or a location relating to a user.

10. The method of claim 8, further comprising:

determining, based on the respective privacy levels, an anonymization level at which the user information is to be anonymized;

anonymizing the user information according to the determined anonymized level; and

providing the anonymized user information to the first service provider and the second service provider.

11. The method of claim 10, further comprising anonymizing the user information via a k-anonymity or a t-closeness process.

12. The method of claim 8, further comprising:

determining a maximum privacy level for the respective privacy levels, wherein the maximum privacy level corresponds to an accuracy of the user information.

13. The method of claim 12, wherein an effectiveness of the services to be included by the first service provider and the second service provider is based on the accuracy of the user information.

14. The method of claim 8, further comprising:

receiving the indication of the respective privacy level to use for the respective service provider via a high level user interface.

15. A system for managing multi-level privacy protection, comprising:

a first service provider defining a first template, wherein the first template comprises a first privacy level and a second privacy level;

a second service provider defining a second template, wherein the second template comprises a third privacy level and a fourth privacy level;

wherein respective privacy levels are associated with respective levels of privacy to maintain for user information; and

a device for managing multi-level privacy protection, comprising a processor configured to:

receive the first template and the second template;

determine, for the respective privacy levels, a respective service that is available or a respective service that is not available, wherein the determination is based on an associated template from an associated service provider;

provide an indication of the respective service that is available or the respective service that is not available for the respective privacy levels;

receive an indication of a respective privacy level to use for a respective service provider; and

coordinate a user interaction with the respective service provider and maintain the indicated respective privacy level associated with the respective service provider.

16. The system of claim 15, wherein the user information is associated with an activity or a location relating to a user.

17. The system of claim 15, wherein the processor of the device for managing multi-level privacy protection is further configured to:

    determine, based on the respective privacy levels, an anonymization level at which the user information is to be anonymized;

    anonymize the user information according to the determined anonymized level; and

    provide the anonymized user information to the first service provider and the second service provider.

18. The system of claim 17, wherein the user information is anonymized via a k-anonymity or a t-closeness process.

19. The system of claim 15, wherein the processor of the device for managing multi-level privacy protection is further configured to:

    determine a maximum privacy level for the respective privacy levels, wherein the maximum privacy level corresponds to an accuracy of the user information.

20. The system of claim 19, wherein an effectiveness of the services to be included by the first service provider and the second service provider is based on the accuracy of the user information.

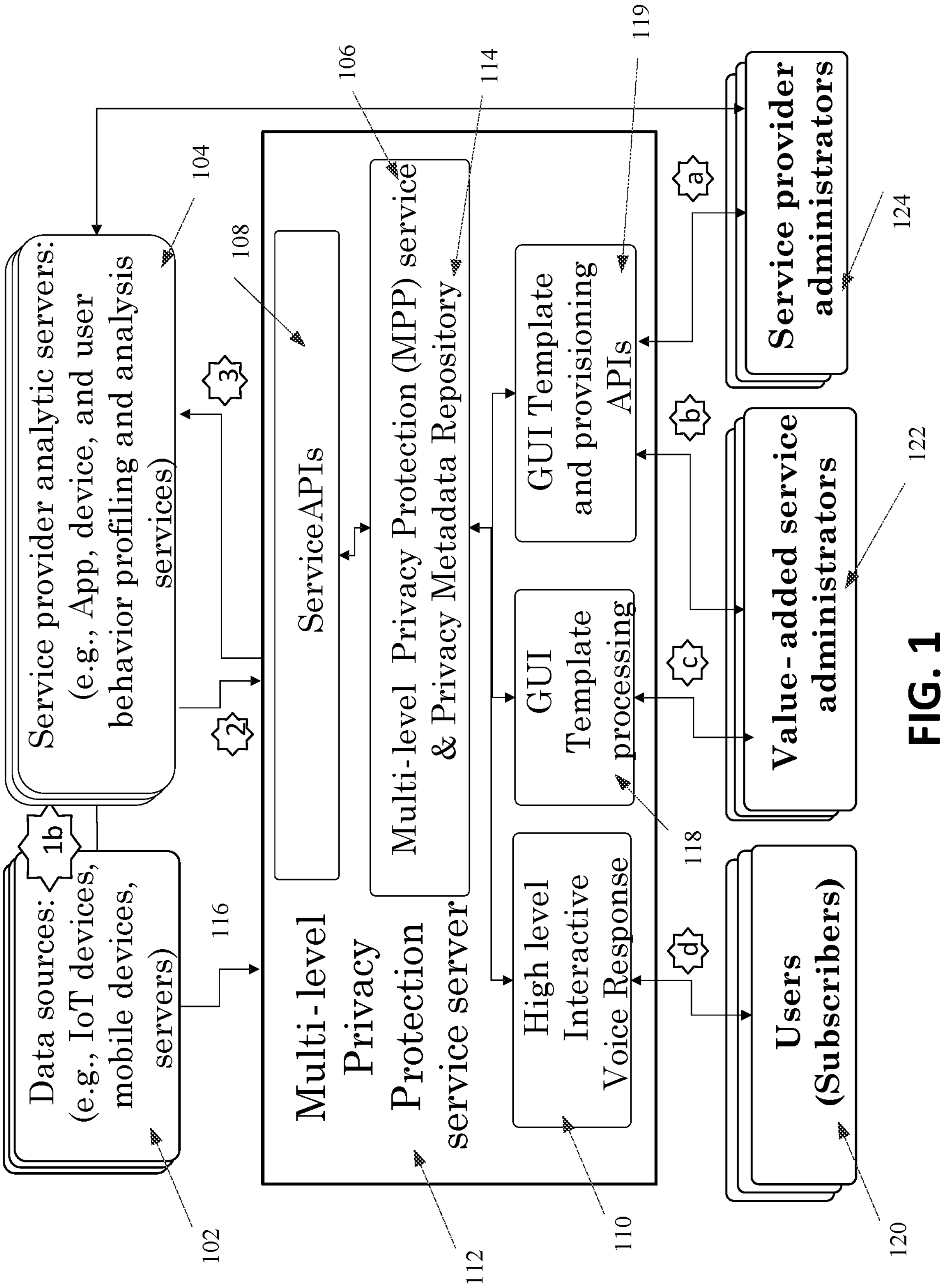

Data sources: (e.g., IoT devices, mobile devices, servers)
102
1b
Service provider analytic servers: (e.g., App, device, and user behavior profiling and analysis services)
104
116
2
3
Multi-level Privacy Protection service server
112
ServiceAPIs
108
Multi-level Privacy Protection (MPP) service & Privacy Metadata Repository
106
114
High level Interactive Voice Response
110
GUI Template processing
118
GUI Template and provisioning APIs
119
a
b
c
d
Users (Subscribers)
120
Value-added service administrators
122
Service provider administrators
124

FIG. 1

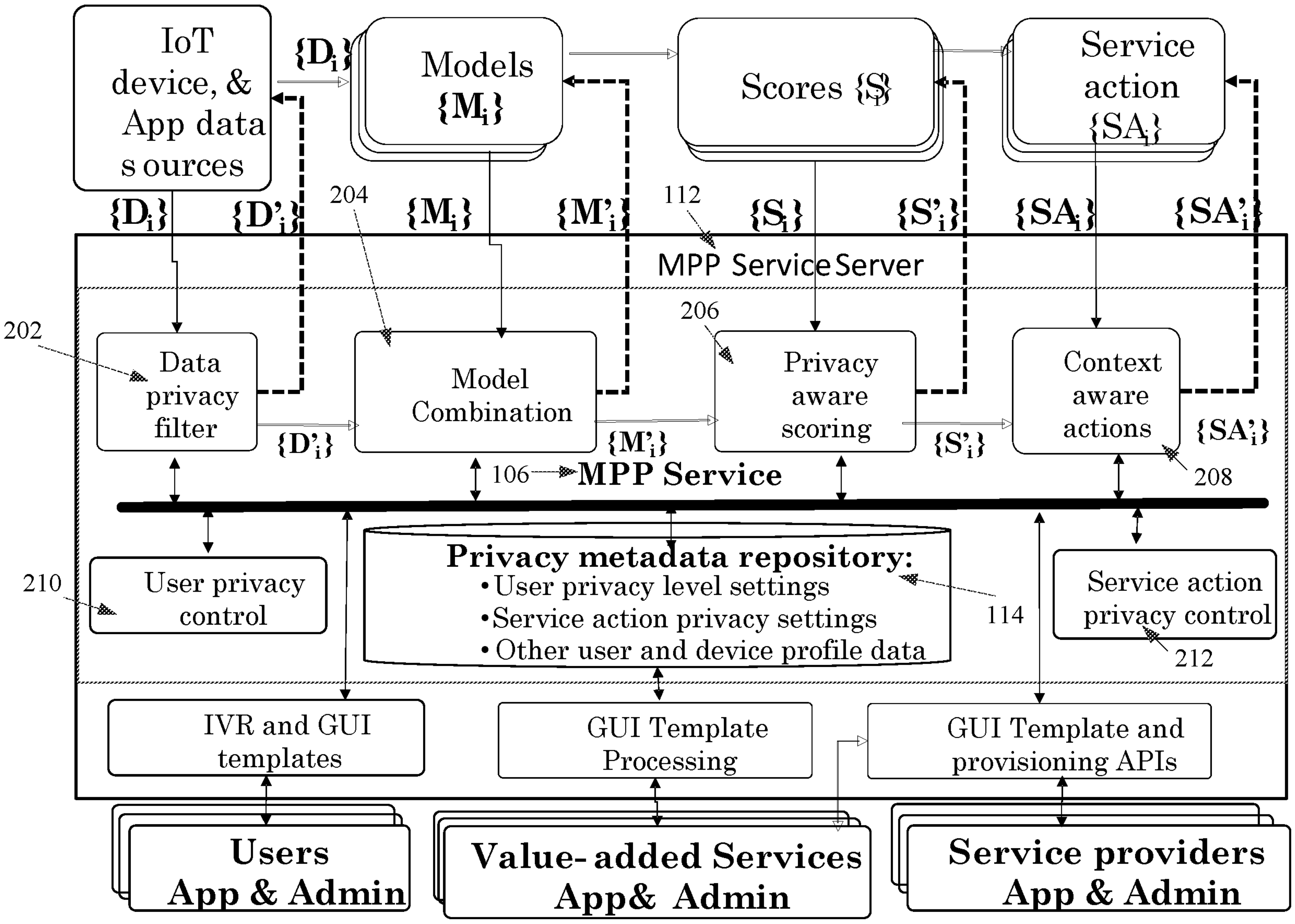

IoT device, & App data s ources
{D_i}
Models {M_i}
Scores {S_i}
Service action {SA_i}
{D_i}
{D'_i}
204
{M_i}
{M'_i}
112
{S_i}
{S'_i}
{SA_i}
{SA'_i}
MPP Service Server
202
Data privacy filter
Model Combination
206
Privacy aware scoring
Context aware actions
{D'_i}
{M'_i}
{S'_i}
{SA'_i}
106
MPP Service
208
210
User privacy control
Privacy metadata repository:
• User privacy level settings
•Service action privacy settings
• Other user and device profile data
114
Service action privacy control
212
IVR and GUI templates
GUI Template Processing
GUI Template and provisioning APIs
Users App & Admin
Value- added Services App& Admin
Service providers App & Admin

FIG. 2

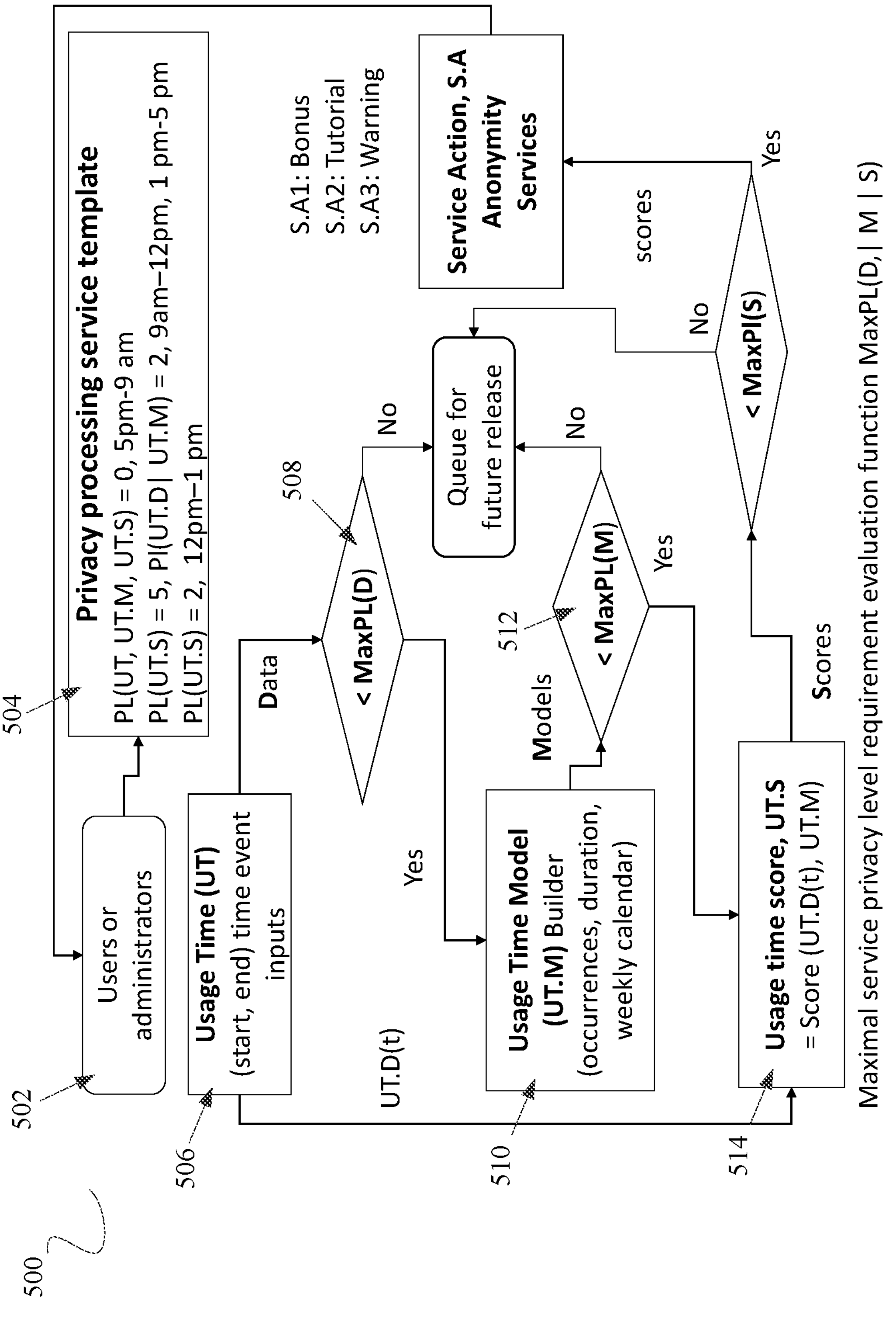
300

302	304	306	308	310	312	314	316	318
User ID	(e.g., Mobile Aps, Sensors, Games)	Activity ID (Activity types and tasks the users is engaging in)	Data type of each analysis stage	Sample data	Time	Location	Privacy Level	Others
UID1	AppID 1 (e.g., Fb | Blog | Fitness | Traffic | others)	Activity 1, [exercise | shopping | biking | travel | others]	Raw data	sessions, vital sign, scores,…	off-hour,	Home	3	
						Train	3	
					work-hour	Office	5	
						others	5	
			Model	Avg/Std	off-hour,	Home	3	
						Train	3	
					work-hour	Office	5	
						others	5	
			Score	%tile Rank	Off-hour	Home	1	
						Train	1	
					work-hour	Office	5	
						others	5	
	AppID 2							
UID2	AppID 2 (e.g., fb)	Activity 2	…	…				

FIG. 3

Service ID	Service Action Type	Privacy Level (Data)	Privacy Level (Model)	Privacy Level (Score)	Service Anony-mity	Rating (by users)	Effective-ness
Grand Theft Auto	Tutorials, Bonus, Weapons,	3	2	5	3	4	3
Shopping service	Bonus, Shopping cart.	4	2	3	5	3	4
Facebook	Sticker, Free game points.	4	2	4	4	5	3
Medical Service	Vital Sign, Medical record	5	3	5	5	5	5
Others							

FIG. 4



Maximal service privacy level requirement evaluation function MaxPL(D,| M | S)

FIG. 5

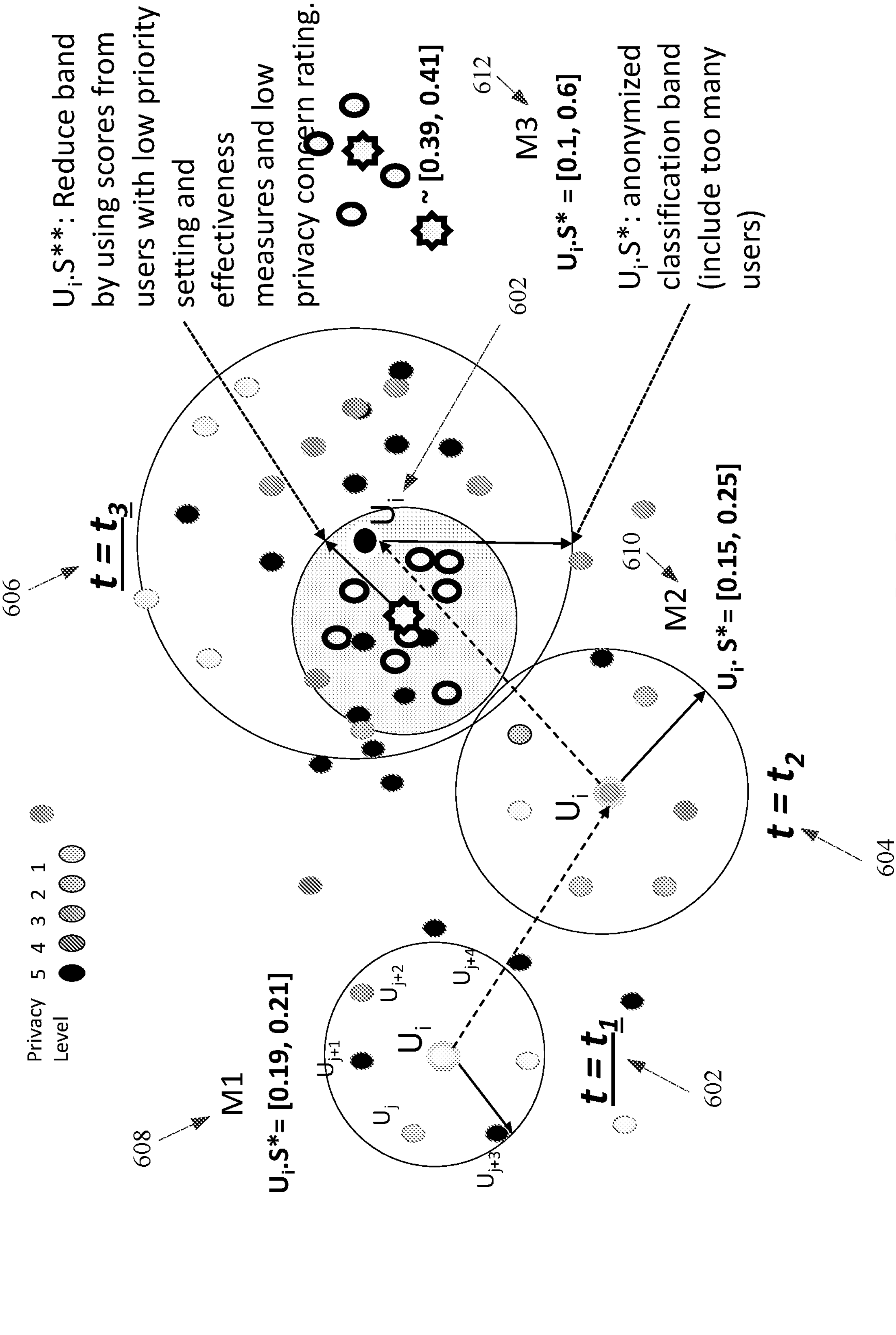

Privacy Level 5 4 3 2 1
● ▨ ▨ ▨ ○
608
M1
$U_i.S^* = [0.19, 0.21]$
U_i
U_j
U_{j+1}
U_{j+2}
U_{j+3}
U_{j+4}
$t = t_1$
602
$t = t_2$
604
U_i
M2
610
$U_i. S^* = [0.15, 0.25]$
$t = t_3$
606
U_i
602
$U_i.S^{**}$: Reduce band by using scores from users with low priority setting and effectiveness measures and low privacy concern rating.
~ [0.39, 0.41]
612
M3
$U_i.S^* = [0.1, 0.6]$
$U_i.S^*$: anonymized classification band (include too many users)

FIG. 6

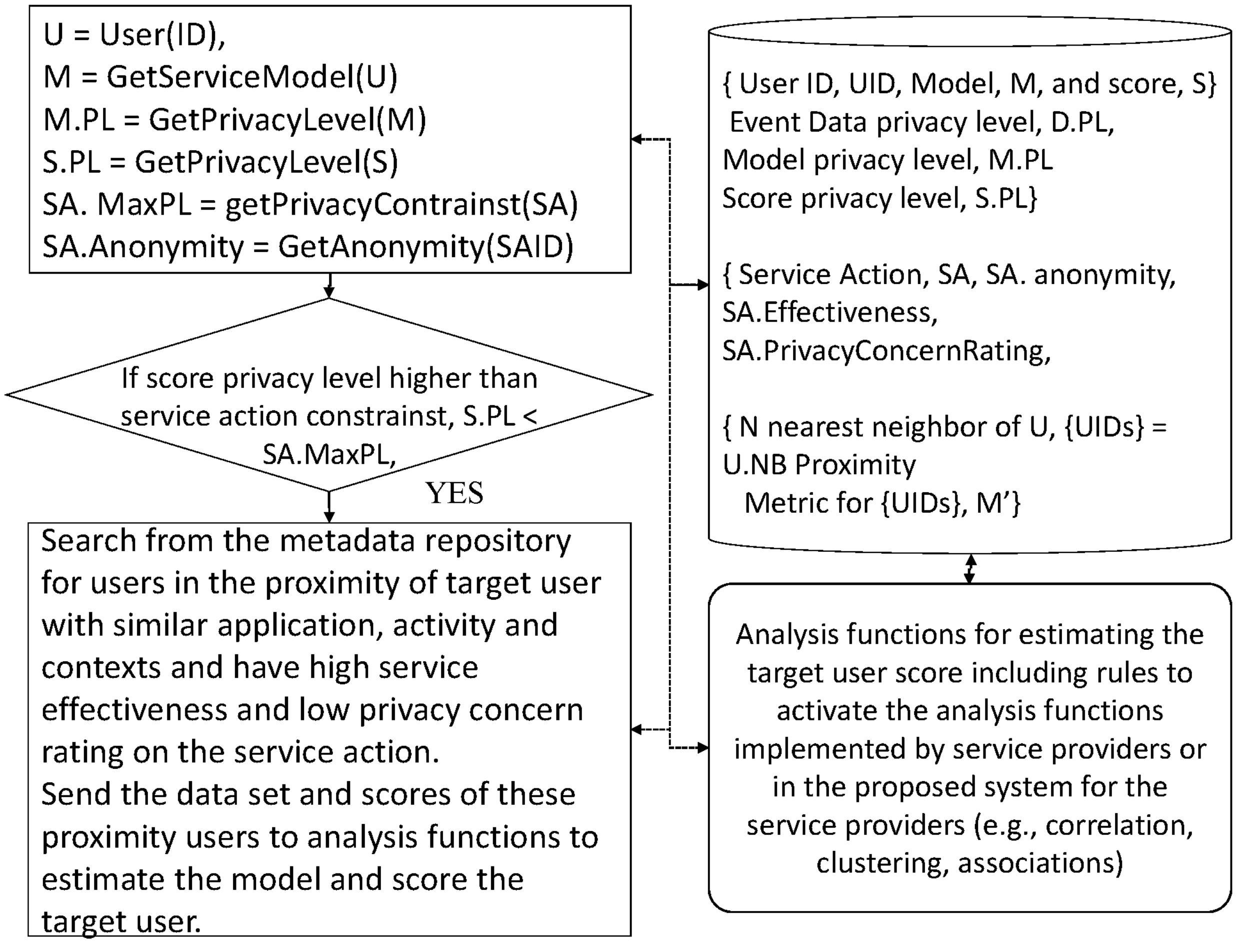
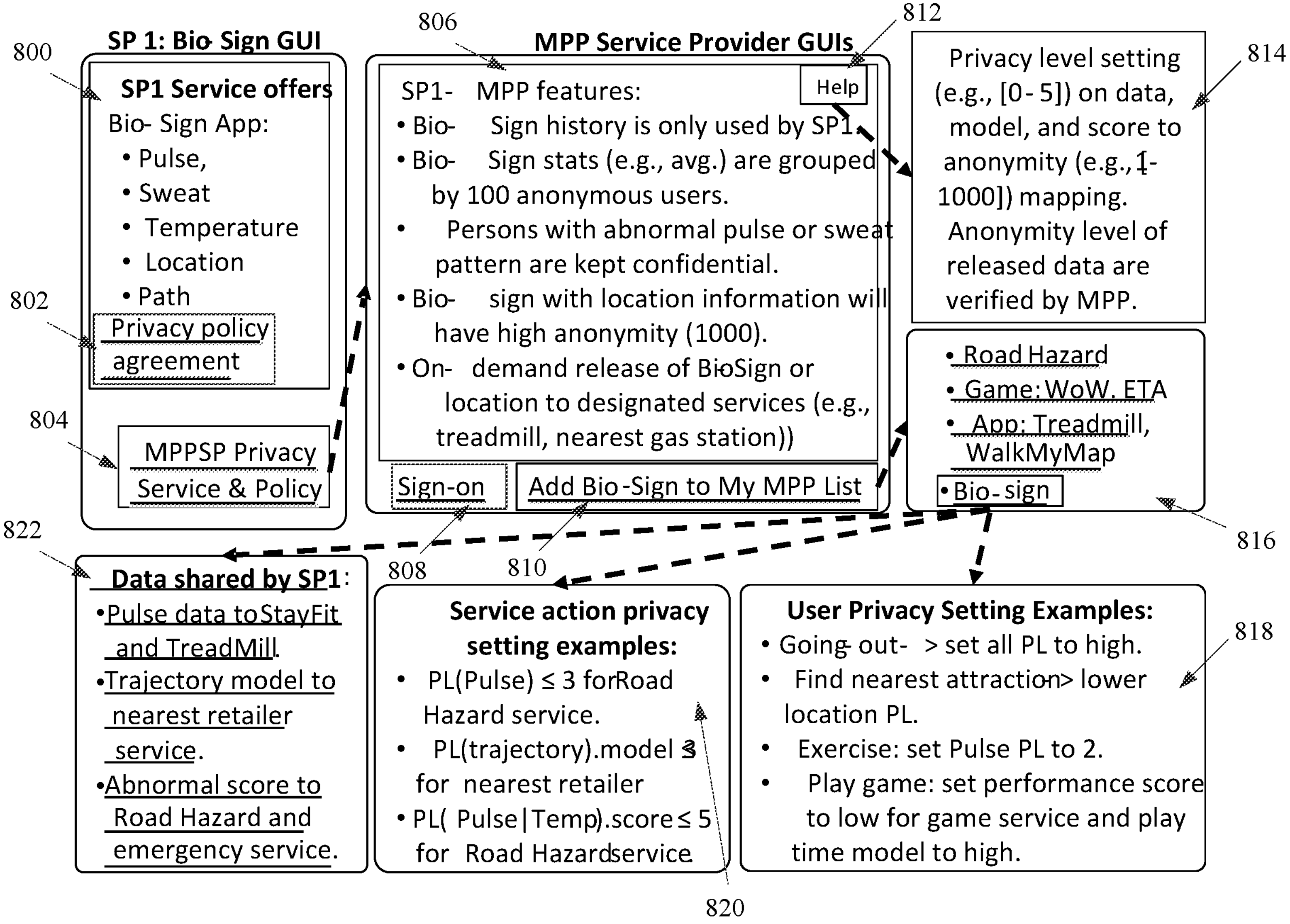

U = User(ID),
M = GetServiceModel(U)
M.PL = GetPrivacyLevel(M)
S.PL = GetPrivacyLevel(S)
SA. MaxPL = getPrivacyContrainst(SA)
SA.Anonymity = GetAnonymity(SAID)
If score privacy level higher than service action constrainst, S.PL < SA.MaxPL,
YES
Search from the metadata repository for users in the proximity of target user with similar application, activity and contexts and have high service effectiveness and low privacy concern rating on the service action.
Send the data set and scores of these proximity users to analysis functions to estimate the model and score the target user.
{ User ID, UID, Model, M, and score, S}
Event Data privacy level, D.PL,
Model privacy level, M.PL
Score privacy level, S.PL}
{ Service Action, SA, SA. anonymity,
SA.Effectiveness,
SA.PrivacyConcernRating,
{ N nearest neighbor of U, {UIDs} =
U.NB Proximity
Metric for {UIDs}, M'}
Analysis functions for estimating the target user score including rules to activate the analysis functions implemented by service providers or in the proposed system for the service providers (e.g., correlation, clustering, associations)

FIG. 7



SP 1: Bio Sign GUI

SP1 Service offers

Bio- Sign App:

- Pulse,
- Sweat
- Temperature
- Location
- Path

Privacy policy agreement

MPPSP Privacy Service & Policy

MPP Service Provider GUIs

SP1- MPP features:

- Bio- Sign history is only used by SP1.
- Bio- Sign stats (e.g., avg.) are grouped by 100 anonymous users.
- Persons with abnormal pulse or sweat pattern are kept confidential.
- Bio- sign with location information will have high anonymity (1000).
- On- demand release of BioSign or location to designated services (e.g., treadmill, nearest gas station))

Help

Sign-on

Add Bio-Sign to My MPP List

Privacy level setting (e.g., [0- 5]) on data, model, and score to anonymity (e.g., [1- 1000]) mapping. Anonymity level of released data are verified by MPP.

- Road Hazard
- Game: WoW, ETA
- App: Treadmill, WalkMyMap
- Bio- sign

Data shared by SP1:

- Pulse data toStayFit and TreadMill.
- Trajectory model to nearest retailer service.
- Abnormal score to Road Hazard and emergency service.

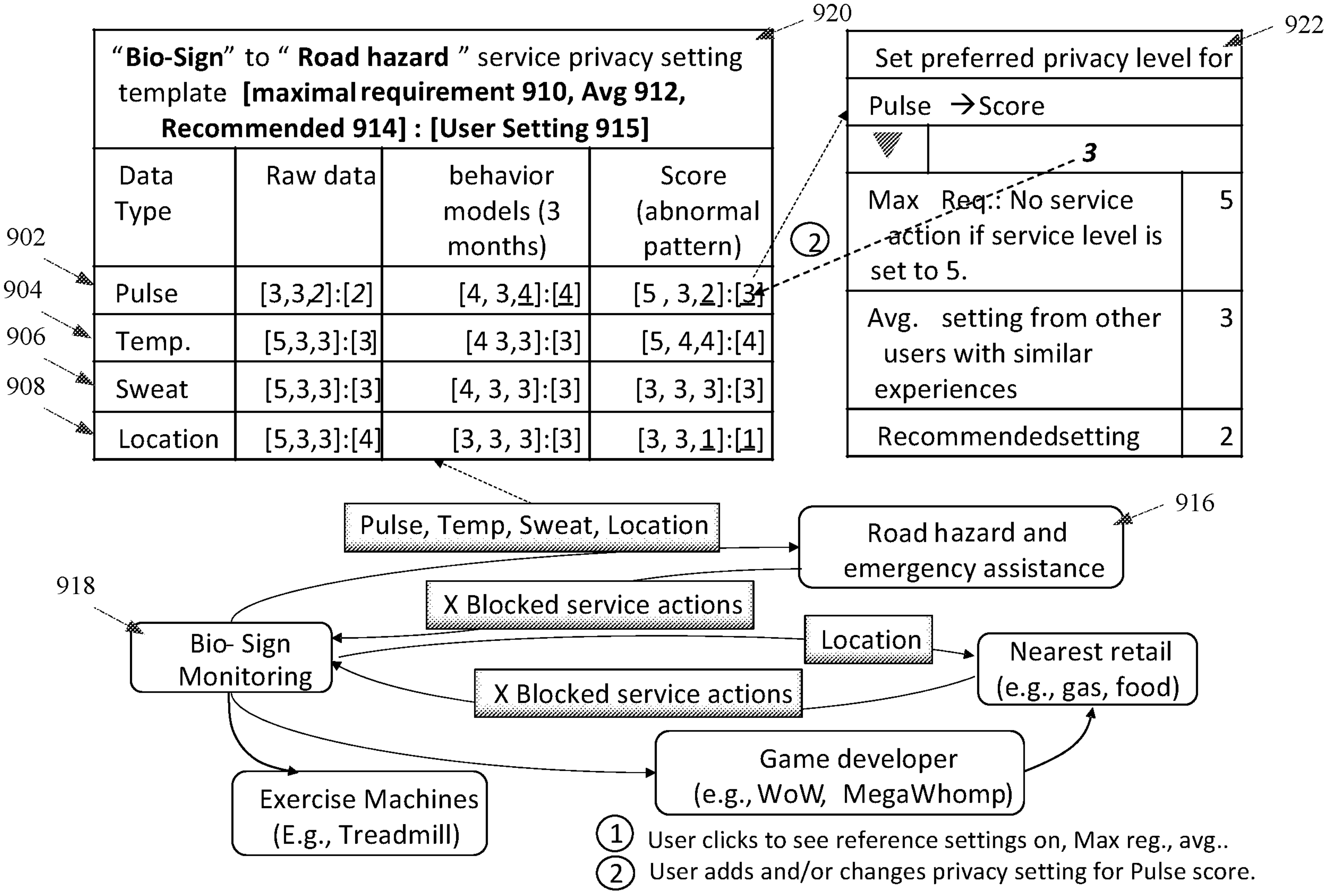
Service action privacy setting examples:

- PL(Pulse) ≤ 3 forRoad Hazard service.
- PL(trajectory).model ≤ 3 for nearest retailer
- PL(Pulse|Temp).score ≤ 5 for Road Hazardservice.

User Privacy Setting Examples:

- Going- out- > set all PL to high.
- Find nearest attraction-> lower location PL.
- Exercise: set Pulse PL to 2.
- Play game: set performance score to low for game service and play time model to high.

FIG. 8



“**Bio-Sign**” to “ **Road hazard** ” service privacy setting template **[maximal requirement 910, Avg 912, Recommended 914] : [User Setting 915]**

Data Type	Raw data	behavior models (3 months)	Score (abnormal pattern)
Pulse	[3,3,2]:[2]	[4, 3,4]:[4]	[5 , 3,2]:[3]
Temp.	[5,3,3]:[3]	[4 3,3]:[3]	[5, 4,4]:[4]
Sweat	[5,3,3]:[3]	[4, 3, 3]:[3]	[3, 3, 3]:[3]
Location	[5,3,3]:[4]	[3, 3, 3]:[3]	[3, 3,1]:[1]

Set preferred privacy level for	
Pulse →Score	
▼	3
Max Req.: No service action if service level is set to 5.	5
Avg. setting from other users with similar experiences	3
Recommendedsetting	2

920
922
902
904
906
908
②
Pulse, Temp, Sweat, Location
Road hazard and emergency assistance
916
918
X Blocked service actions
Bio- Sign Monitoring
Location
Nearest retail (e.g., gas, food)
X Blocked service actions
Game developer (e.g., WoW, MegaWhomp)
Exercise Machines (E.g., Treadmill)

① User clicks to see reference settings on, Max reg., avg..
② User adds and/or changes privacy setting for Pulse score.

FIG. 9

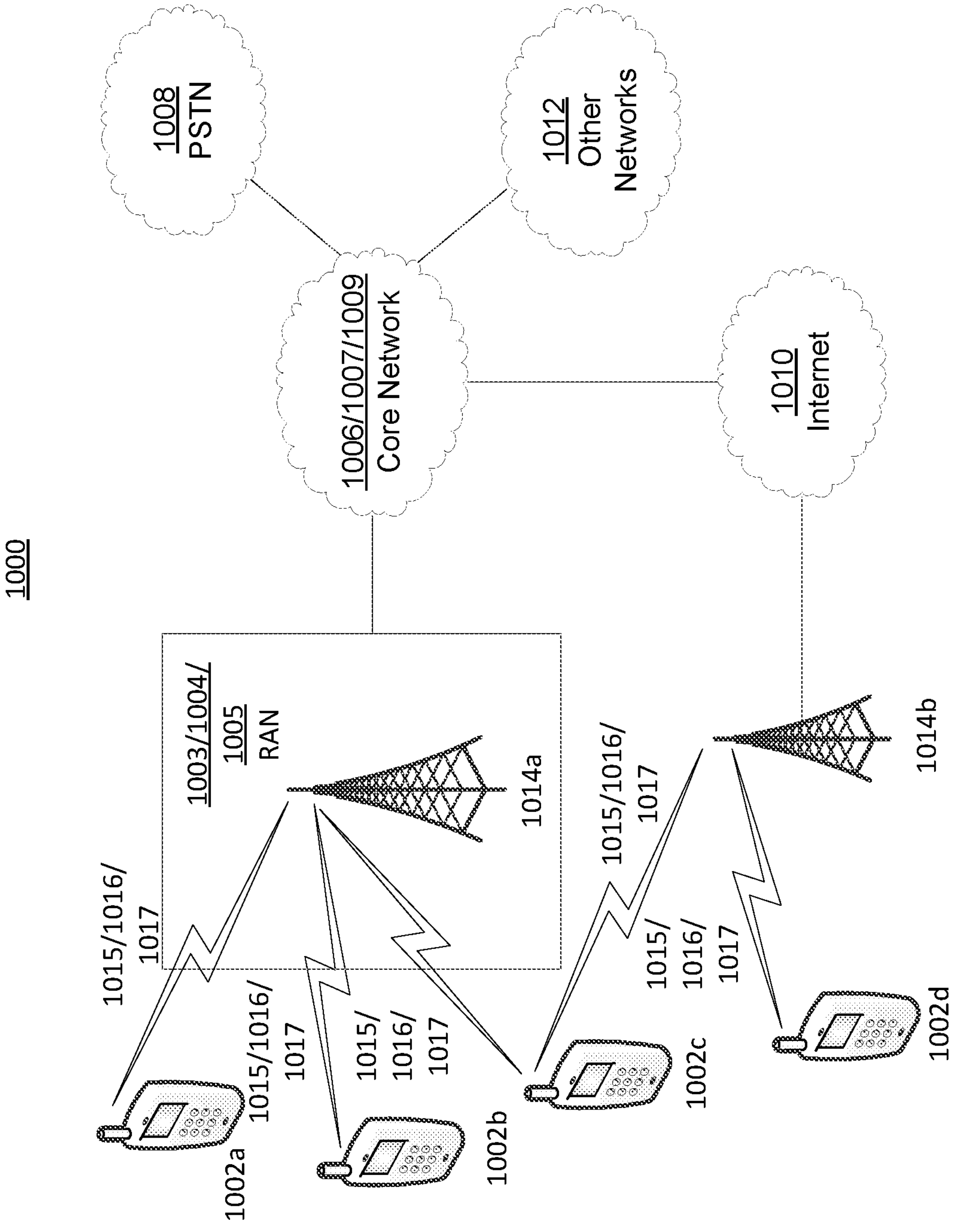

1000
1003/1004/
1005
RAN
1006/1007/1009
Core Network
1008
PSTN
1012
Other
Networks
1010
Internet
1014a
1014b
1015/1016/
1017
1015/1016/
1017
1015/
1016/
1017
1015/1016/
1017
1015/
1016/
1017
1002a
1002b
1002c
1002d

FIG. 10A

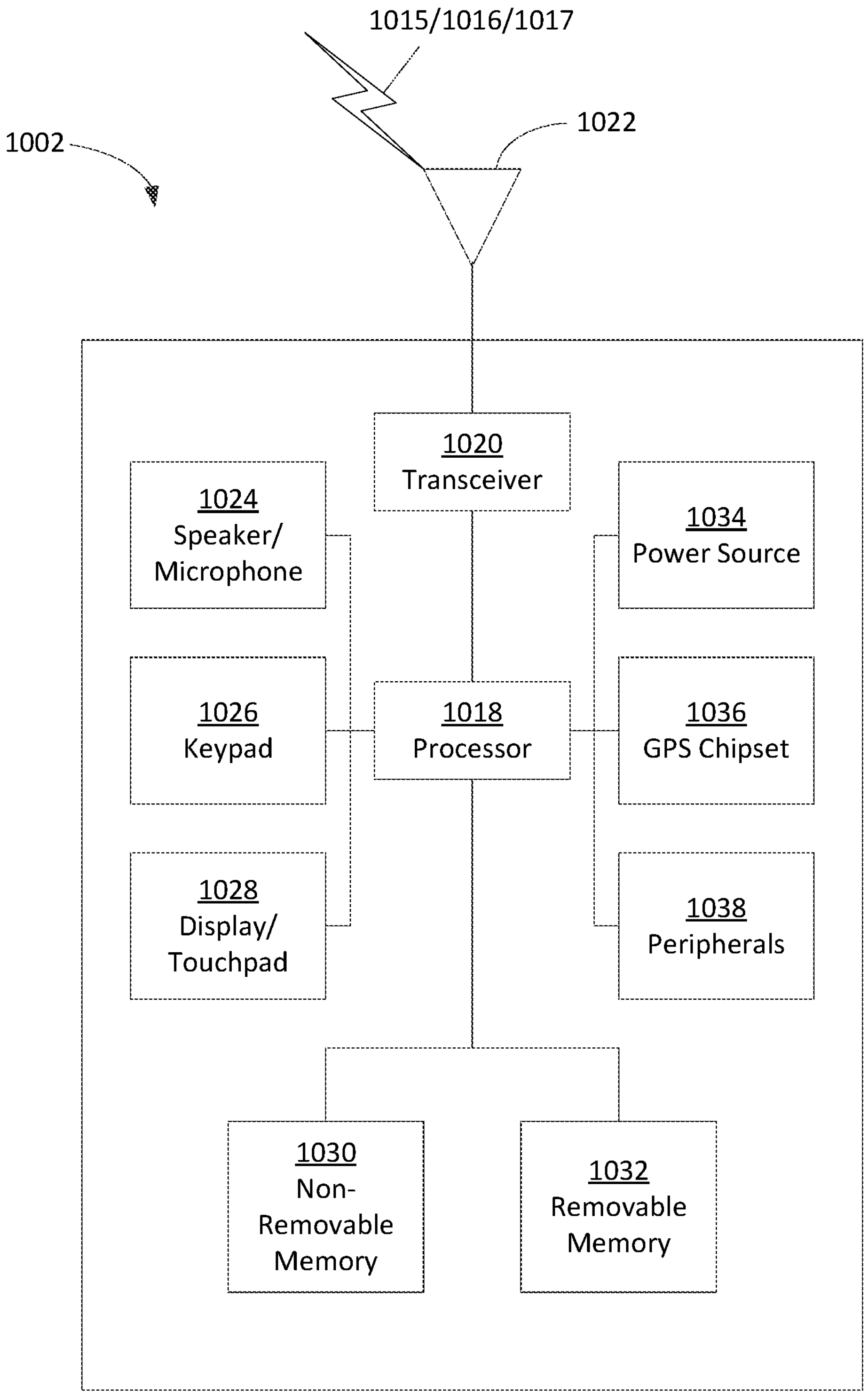

1015/1016/1017
1002
1022
1020
Transceiver
1024
Speaker/
Microphone
1026
Keypad
1028
Display/
Touchpad
1018
Processor
1034
Power Source
1036
GPS Chipset
1038
Peripherals
1030
Non-
Removable
Memory
1032
Removable
Memory

FIG. 10B

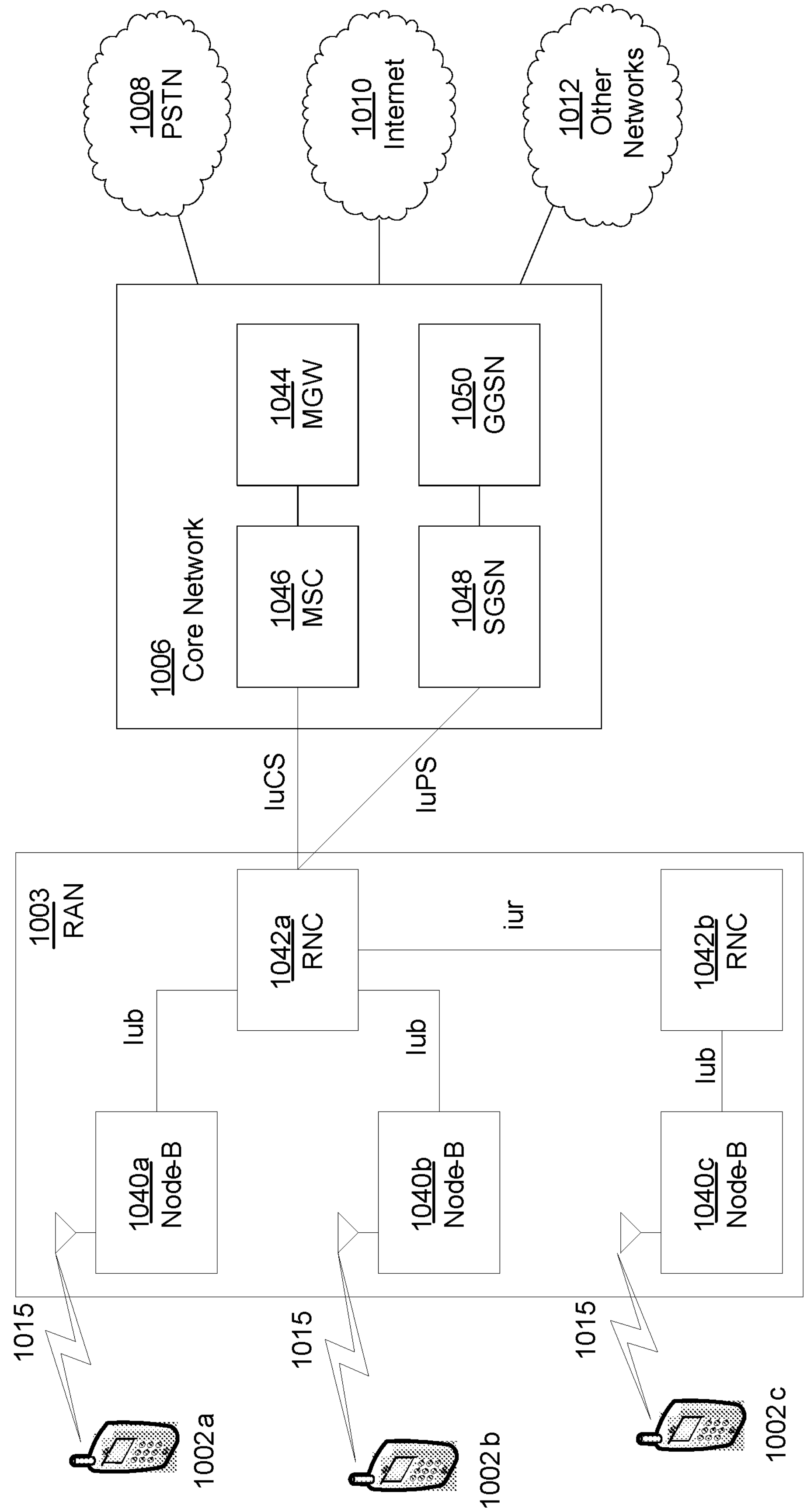

1008
PSTN
1010
Internet
1012
Other
Networks
1006
Core Network
1044
MGW
1046
MSC
1050
GGSN
1048
SGSN
IuCS
IuPS
1003
RAN
1042a
RNC
iur
1042b
RNC
Iub
Iub
Iub
1040a
Node-B
1040b
Node-B
1040c
Node-B
1015
1015
1015
1002a
1002b
1002c

FIG. 10C

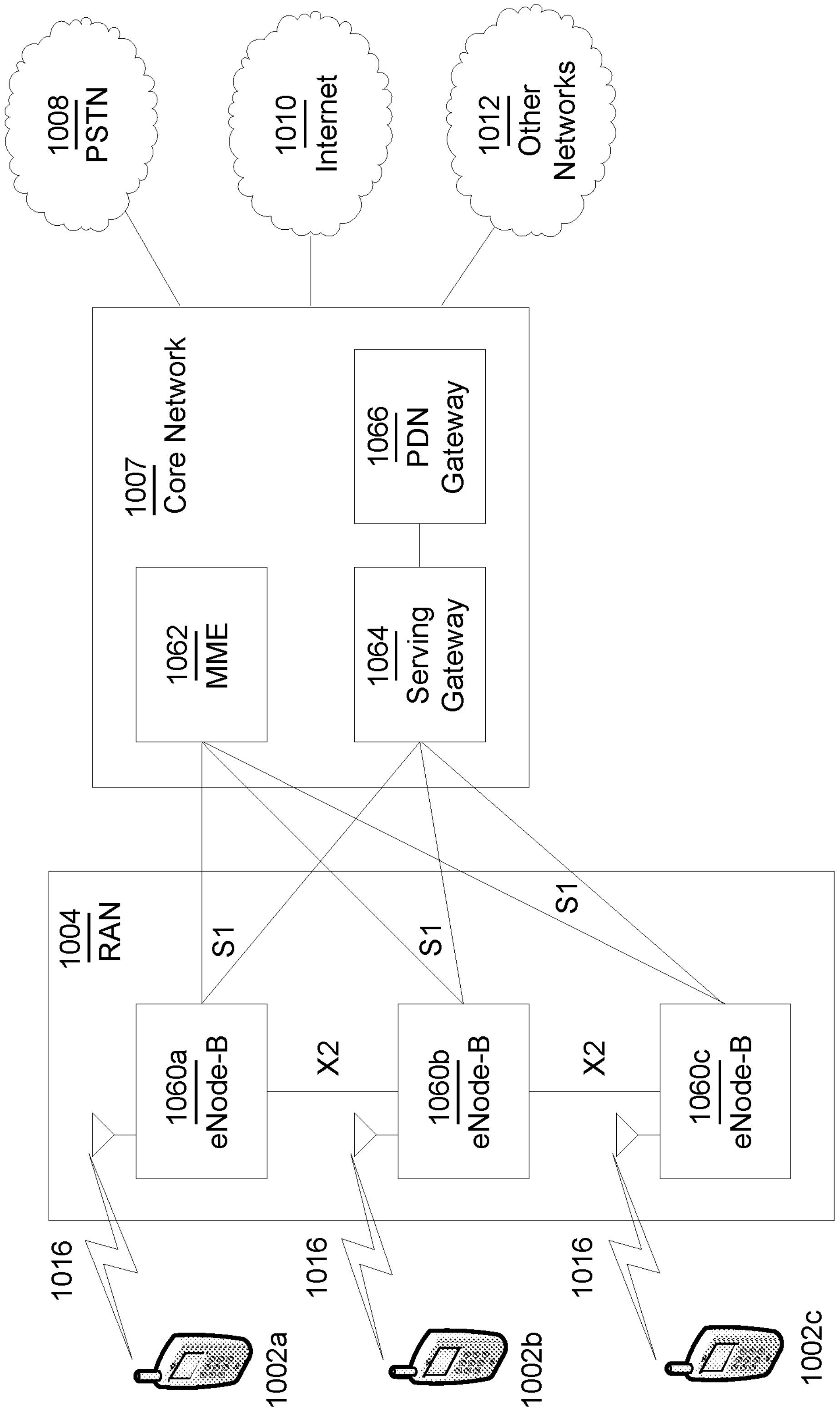

1008
PSTN
1010
Internet
1012
Other
Networks
1007
Core Network
1062
MME
1064
Serving
Gateway
1066
PDN
Gateway
1004
RAN
S1
S1
S1
1060a
eNode-B
1060b
eNode-B
1060c
eNode-B
X2
X2
1016
1016
1016
1002a
1002b
1002c

FIG. 10D

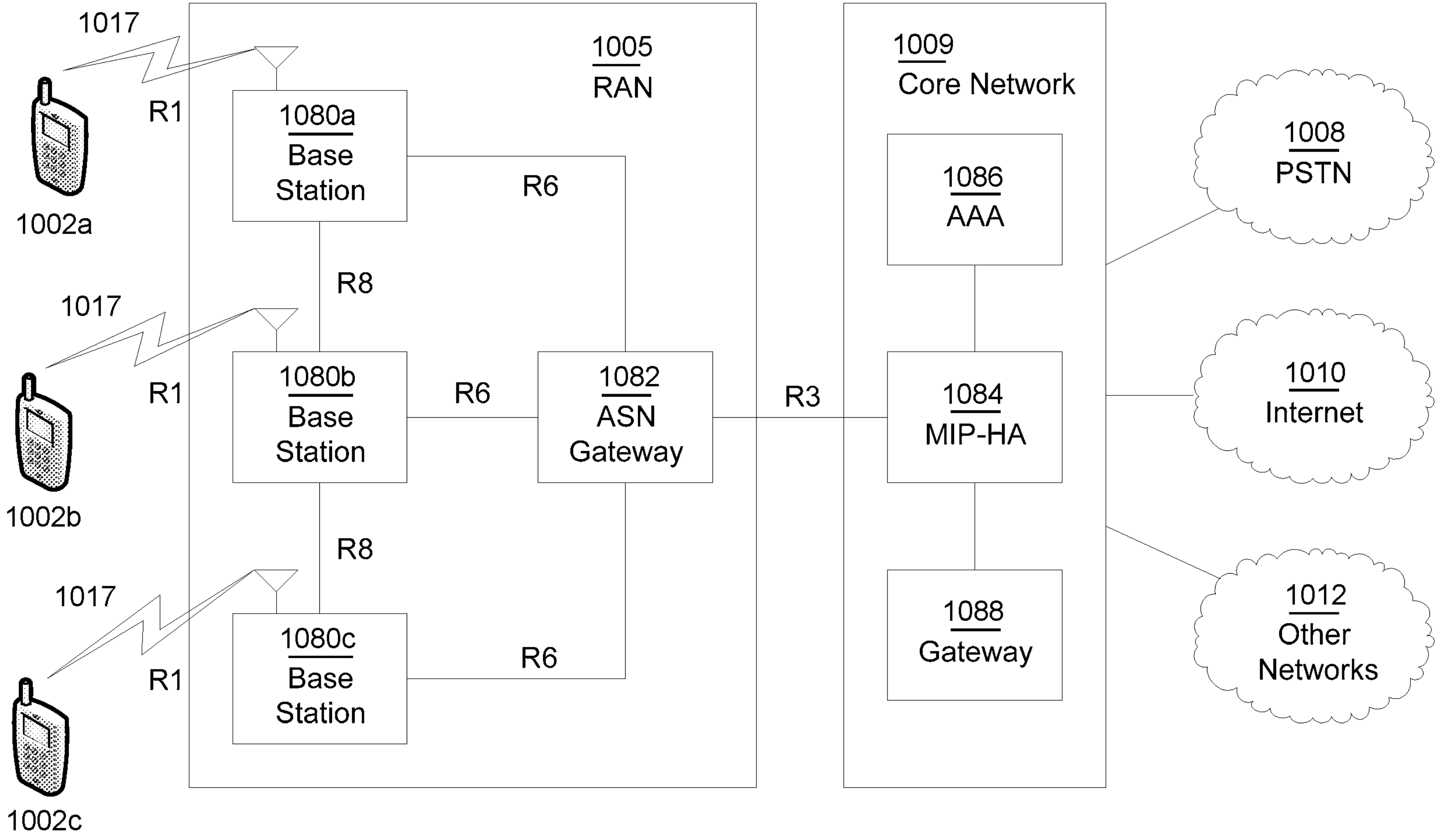

1017
1002a
R1
1017
1002b
R1
1017
1002c
R1
1005
RAN
1080a
Base
Station
1080b
Base
Station
1080c
Base
Station
R8
R8
R6
R6
R6
1082
ASN
Gateway
R3
1009
Core Network
1086
AAA
1084
MIP-HA
1088
Gateway
1008
PSTN
1010
Internet
1012
Other
Networks

FIG. 10E

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/055719

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L29/08 H04W12/02
ADD. H04W4/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L H04W G01D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2012/149981 A1 (NOKIA SIEMENS NETWORKS OY [FI]; ROOKE MICHAEL JOHN [FI]) 8 November 2012 (2012-11-08) abstract; figures 1, 2 page 1, line 10 - line 16 page 2, lines 9-12, 31-36 page 3, line 1 - line 30 page 4, lines 9-19, 29 - page 5, line 27 page 6, line 12 - line 31 page 9, line 6 - line 31 page 34, line 30 - page 35, line 19 -----	1-20
A	US 2012/329384 A1 (BOLDYREV SERGEY [FI] ET AL) 27 December 2012 (2012-12-27) abstract; figures 1, 4B, 4C, 4D paragraphs [0004] - [0015], [0078] - [0085] ----- -/--	1-20

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 30 November 2016	Date of mailing of the international search report 08/12/2016
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Hristova, Ana

1

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2014/047551 A1 (NAGASUNDARAM SEKHAR [US] ET AL) 13 February 2014 (2014-02-13) abstract; figures 1-4, 6, 7 paragraphs [0005] - [0014], [0043], [0046], [0058] - [0073] -----	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2016/055719

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2012149981 A1	08-11-2012	EP 2705333 A1 WO 2012149981 A1	12-03-2014 08-11-2012
US 2012329384 A1	27-12-2012	US 2012329384 A1 US 2014293928 A1 WO 2013001148 A1	27-12-2012 02-10-2014 03-01-2013
US 2014047551 A1	13-02-2014	NONE	