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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 April 2009 (09.04.2009)

PCT

(10) International Publication Number
WO 2009/046389 A1

(51) International Patent Classification:
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/US2008/078866

(22) International Filing Date: 3 October 2008 (03.10.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/977,371	3 October 2007 (03.10.2007)	US
61/099,736	24 September 2008 (24.09.2008)	US

(71) Applicant *(for all designated States except US)*: **PURDUE RESEARCH FOUNDATION** [US/US]; Office Of Technology Commercialization, Purdue Research Park, 3000 Kent Avenue, West Lafayette, IN 47906 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **GHAFOOR, Arif** [US/US]; 3409 Morgan Street, West Lafayette, IN 47906 (US). **SAMUEL, Arjmand, M.** [US/US]; 206-15 Airport Road, West Lafayette, IN 47906 (US).

(74) Agent: **SCHANTZ, Matthew, R.**; Bingham Mchale Llp, 10 West Market Street, 2700 Market Tower, Indianapolis, IN 46204 (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, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(54) **Title:** COMPOSING AND ENFORCING CONTEXT-AWARE DISCLOSURE RULES FOR PRESERVING PRIVACY AND SECURITY OF INFORMATION

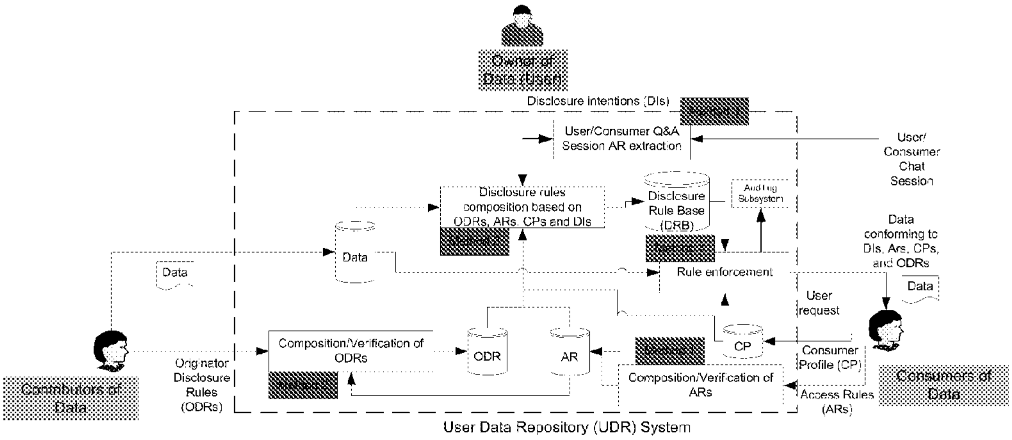

Owner of Data (User)
Disclosure intentions (DIs)
User/Consumer Q&A Session AR extraction
User/ Consumer Chat Session
Disclosure rules composition based on ODRs, ARs, CPs and DIs
Disclosure Rule Base (DRB)
Auditing Subsystem
Data conforming to DIs, Ars, CPs, and ODRs
Data
Data
Rule enforcement
Data
User request
Composition/Verification of ODRs
ODR
AR
CP
Consumer Profile (CP)
Composition/Verification of ARs
Access Rules (ARs)
Contributors of Data
Originator Disclosure Rules (ODRs)
Consumers of Data
User Data Repository (UDR) System

Fig. 7

(57) **Abstract:** This document provides details of some embodiments of the proposed system and methods. An example system is explained with the help of example applications and implementations. The technical details of the methods are augmented with the help of diagrams and examples. Today, an increasing number of users are turning to the internet to manage their personal information regarding finances, credit, healthcare, travel, investments, employment history, etc.This trend is further being fueled by an ever-growing number of companies and government agencies such as banks, hospitals and employers, managing users' personal information in some form of online applications and databases. The aim is to save time and money by streamlining and facilitating access to and manipulation of information online using the internet/intranet both in fixed and mobile environments.

Composing and Enforcing Context-Aware Disclosure Rules for Preserving Privacy and Security of Information

BACKGROUND

This document provides details of some embodiments of the proposed system and methods. An example system is explained with the help of example applications and implementations. The technical details of the methods are augmented with the help of diagrams and examples.

Today, an increasing number of users are turning to the internet to manage their personal information regarding finances, credit, healthcare, travel, investments, employment history, etc. This trend is further being fueled by an ever-growing number of companies and government agencies such as banks, hospitals and employers, managing users' personal information in some form of online applications and databases. The aim is to save time and money by streamlining and facilitating access to and manipulation of information online using the internet/intranet both in fixed and mobile environments.

SUMMARY

The following description is not in any way to limit, define or otherwise establish the scope of legal protection sought. In general terms, the disclosed technology relates to a system for controlling dissemination of a user's private data. Context-aware disclosure rules are generated by an individual to convey his or her desires regarding disclosure of his or her personal information. These rules are then composed and applied to control disclosure of that information and provide feedback for further development of the rule set.

Further objects, embodiments, forms, benefits, aspects, features and advantages of the disclosed technology may be obtained from the description, drawings, and claims provided herein.

DESCRIPTION

A case in point is the emerging Personal Health Record (PHR) technology which allows users the full-ownership of their Electronic Health Records (EHR) in terms of access, management and sharing of their data across multiple healthcare providers (e.g. clinical practices, hospitals, pharmacies, etc.). The key challenge behind such applications is to empower a user to control his or her private information not only in terms of management and access but also allowing the sharing of their information with others whom they authorize, in a private, secure and confidential environment. The key tenet of such information sharing is that the decision to disclose personal information should rest entirely with the user. One of the key barriers to wider use of such applications is the inability of the user to define context-aware disclosure and sharing rules for a collection of information from dispersed sources in a user friendly and consistent manner. Context is defined as “any information that can be used to characterize the situation of an entity”. For example time of day of a certain activity is a context parameter for that activity. Similarly, location of activity is also one of the context parameters. One example of the proposed system to support a privacy preserving PHR is depicted in Fig. 1. Note that the healthcare providers (hospitals, physicians, etc) consume information held in the PHR as well as contribute to this information. The User who is the owner of all information held in the PHR composes disclosure rules which are applied to all accesses of information from the PHR.

Another example of storage and use of an individual’s personal information by a large number of users is financial information. While most portions of an individual’s financial information are private, some parts may still be shared with financial institutions, government agencies, advertisers, etc. Data held by credit bureaus include name, social security number, bank account information, credit card accounts, financial history, etc. By utilizing the proposed system, a user (owner of information) may define varying levels of privileges on all financial information, consequently safeguarding his or her privacy. A second example implementation of the proposed system in the financial sector is depicted in Fig. 2.

Another important application of the proposed system is in personalizing an individual's information held in search engines such as Google, Yahoo, etc. By facilitating a user's definition of disclosure rules on search engine data related to him or her, such as phone number, address, etc., a user takes control of who retrieves what, and under what conditions (time, location) from a search engine. An example implementation of the proposed system in the domain of search engines is depicted in Fig. 3.

A large amount of data related to each citizen is also held by the government in the form of tax returns, social security data, automobile registration history, criminal records, etc. The proposed system allows the user to specify disclosure rules on this information and hence exercise control in terms of allowing access to selected information under changing contextual parameters.

Another interesting utility of the proposed system is with internet-based personal networking sites such as myface.com, linkedin.com etc. The proposed system will allow users to define customized disclosure rules for members of their group thus protecting privacy of users who may desire a subset of network peers to view portions of his or her profile information and friend list.

Generally, disclosure of personal information depends on the circumstances of access including the privacy concerns of the individual user. In particular, for using any internet-based service dealing with a user's personal information, the overriding concern is ensuring security and privacy of their personal information. Access to critical data depends on users' identity as well as environmental parameters such as time and location. While temporal based access control models are well suited for enforcing access control decisions on fixed users, they loose their effectiveness when users employing handheld computing devices are mobile and move from a secure locale to an insecure one, or vice versa.

An overview of location discovery is given in [3]. Sensing location context accurately and reliably is at the core of applying spatial constraints in the computing environment. A number of techniques have been reported and can be divided into two broad categories, namely: outdoors and indoors. The obvious choice for outdoor sensing of location is the Global Positioning System (GPS) [5]. GPS enables a cheap and accurate means of acquiring longitude, latitude and altitude by using time of flight and geometry of satellite transmitters as a basis of calculations. The accuracy of GPS has recently been further enhanced with the US Government turning off the degradation of the civilian data streams from the satellites. As GPS signals cannot be received indoors, a number of indoor location sensing techniques have been proposed. Notable among them the Olivetti Active Badge System [6], Xerox ParcTab [7] and the Cyberguide project [8].

Physical location is the most widely used representation for location and can be divided into symbolic and geometric representations. Symbolic location can include names of places (Miami, New York, etc.) as well as names of places by their functions (stadium, mall, etc.). Symbolic location can be represented by using nouns (e.g., name of a city) and hence is easier to implement. However with a large number of symbolic locations it offers a scalability challenge in terms of the number of names that can be given to physical locations.

Geometric location can be represented by using various types of coordinate systems in terms of numbers and elevation etc. In this context physical location can be represented according to three dimensions, namely longitude, latitude and height. Geometric location is more accurate by far and offers higher resolution. It is also universal if the coordinate system is known. However, geometric locations need to be converted to symbolic locations for a user to correctly and conveniently comprehend and use.

Time and additional context parameters such as system load, network characteristics etc. also play an important role in access control decisions. Time has well known semantics and has been thoroughly investigated in an access control environment in [9], among others.

Role Based Access Control (RBAC) has emerged as a de-facto model for specifying security requirements of large organizations. Its strength lies in the definition of user roles more akin to the functional responsibilities of users in the organization and abstracting object permissions as roles [13]. The Generalized Temporal RBAC (GTRBAC) incorporates a set of language constructs for the specification of various contextual constraints such as time [9]. However GTRBAC does not allow the specification of rich spatial constraints in which relationships between spatial contexts affects access control decisions.

The aim of this system is to provide for the composition and enforcement of disclosure rules for personal data held in a User Data Repository (UDR). These rules are specified by the *contributors*, *consumers* and *owner* of data. These users can upload, manage and download information to/in/from the UDR, which may be from remote locations using internet enabled computers, Personal Digital Assistants (PDAs), mobile data access and display devices etc. An overview of an exemplary system is depicted in Fig. 7.

The *contributors* of data are the originators of user data generated as a consequence of the user's physical or other personal interaction with *contributors*. An example in this case is a healthcare provider who generates health-related information concerning a patient (user) and contributes this information to be stored in the UDR. In addition to contributing data, the *contributor* also associates Originator Disclosure Rules (ODRs) with each element of data.

The *consumers* of data are the external entities who may be interested in the accessing data related to a user. These consumers may also be *contributor*s of data. *Consumers* provide Access Rules (ARs) to the UDR defining the access times, locations, and other context parameters that may govern a particular access for generic data types. An example in this regard may be a physician defining the times of day as well as location of access (e.g., from his practice) for viewing pathology reports of a particular user. This access by the physician may be from a remote location using a PDA or an internet enabled mobile device. The consumers also provide their profile information (Consumer Profile (CP)) such as name, credentials and affiliation.

The user, who is the owner of his data held in the UDR, composes disclosure rules based on his or her Disclosure Intentions (DI) (e.g., the physician may see his pathology report from hospital at certain times), ODRs, ARs and CPs. These rules are then stored in the Disclosure Rule Base (DRB). Any access of the user's personal data by the *consumers* is evaluated against the rules in the DRB and appropriate data sent back to the consumer.

Each access by the *consumer* is evaluated by the rule enforcement module (Method 4) based on input from the disclosure rule base. The required data is extracted from the data storage system and sent to the consumer. Each request, either satisfied or denied, is also logged in the auditing subsystem. This allows the *owner* to track access to their personal records as well as evaluate accesses which were not satisfied by the system based in disclosure rules. Additionally, the audit subsystem keeps track of all disclosure rules that allowed access to a certain part of data with a view of facilitating the *owner* to adapt disclosure rules.

A conceptual overview of the proposed system is depicted in Fig. 8.

The following are four methods that enable UDR to maintain privacy and security of data held by it.

Method 1: Composition and verification of Access Rules (ARs) by *consumers* of data held in the User Data Repository.

Method 2: Composition and verification of Originator Disclosure Rules (ODRs) by the *contributor* related to data being contributed to the User Data Repository.

Method 3: Composition and verification of disclosure rules based on ODRs, ARs, and User Intentions (UIs).

Method 4: Enforcement of disclosure rules on access of data from the UDR based on context of request.

Method 5: Extraction of ARs from Question and Answer (Q&A) session between *Owner* and *Consumer*.

Next, we provide details of each method.

Method 1: Composition and verification of Access Rules (ARs) by *consumers* of data held in the User Data Repository.

Consumers of data from a UDR define their access rules in this method (for overall context refer to Fig. 7). Such specification involves defining the rules and verifying if the rules are consistent or not. The method can be broken down into a series of interrelated steps depicted in Fig. 9 and elaborated as follows.

Step 1: The *consumer* is presented a web page to enter his or her personal information. This information will be used to identify a consumer in the UDR and may include name, address, affiliations to organizations (specific to the application for which UDR is being implemented), ranks and status in organizations, etc.

Step 2: The *consumer* is presented a web page from which the *consumer* selects roles. These roles are predefined in the UDR and represent the application domain in which the proposed system is implemented. Examples of pre-defined roles in a PHR implementation could be Primary Physician, Radiologist, etc. A consumer's assignment to specific role implies privileges that will be defined by the *owner* in the disclosure rules (Method 3).

Step 3: The *consumer* enters temporal information for the times and days (of the week or month) that he or she is available to access data from the UDR. This is achieved by selecting from a standard template of times and days presented by the web page to the *consumer*. Entry of this information is optional and if not entered implies that the *consumer* is available at all times and all days.

Step 4: The *consumer* enters locations from which he or she can access the data from the UDR. These locations, together with the temporal information define the spatio-temporal context of access by the *consumer*. Such location may be geometric coordinates of the user (sensed by a GPS receiver) or may by the IP address of the mobile device being used.

Step 5: In this step the *consumer* enters any other contextual parameters such as system properties or environmental conditions under which data is accessed from UDR. As example in this case may be the type of device the *consumer* is using to access data.

Step 6: The entered information is verified for consistency in this step. The properties to be verified are listed in Table 1. Verification is done using standard model checking techniques as discussed in [10, 11, 12]. This step will evaluate the safety and liveness properties and in case of any violations, the user will be presented the correct webpage to make changes.

Step 7: The collected and verified ARs are saved in the database. The resulting rules may be saved, for example, in any one of the following standards: ASCII or Unicode, Text, XML, relational database, etc.

Property No.	Property	Explanation	Type
1	Reachability of Role	No user defined for a role	Safety
2		User selects a role to be part of	Liveness
3	Reachability of Permissions	Permission not granted to a role	Safety
4		Permission granted for a role	Liveness
5	Conflicting Constraints	Define two similar (e.g. temporal or spatial) contextual constraints opposing each other	Safety
6		Define two dissimilar contextual constraints opposing each other	Safety
7	Access Leakage	Same permission (access to same object) associated with roles of different users (*owners*)	Safety
8		Permissions for different users granted to the same role	Safety

Table 1: Sample liveness and safety properties to be used for verification of ARs

In addition to collecting and verifying ARs from the *consumer*, this method also involves entry of profile information by the *consumer*, also called Consumer Profile (CP). This profile information may include such individually identifying information as name, position in an organization, credentials such as membership of an organization etc. The CP is used by the user (in method 3) to compose individualized disclosure rules.

Method 2: Composition and verification of Originator Disclosure Rules (ODRs) by the *contributor* related to data being contributed to the User Data Repository.

Data can be contributed to the UDR electronically as well as manually. Method 2 relates to composition of ODRs related to the data being uploaded to the UDR in electronic format (for overall context refer to Fig. 7). The overall process is depicted in Fig. 10.

Step 1: Data is uploaded to the UDR. The interface provided to the *consumer* for data upload is through a web site. This interface allows upload of data as files in a number of formats such as simple text (with data labels), excel sheets, word documents (with labels conforming to predefined document elements), XML, multimedia content (video, images, etc).

Step 2: Fields from the uploaded document are extracted. This extraction is based on predefined labels in the files.

Step 3: The ARs and CPs collected by the UDR (Method 1) are used in this step to formulate the ODRs composed by the *contributor*. The *contributor* is presented with a user interface (depicted in Fig. 11) which lists all extracted labels (Step 2) and a selectable list of roles, users, time and location (these parameters are retrieved from the AR and CP base). The user select list is driven by the role selected by the user. Similarly, the time and location select lists are also driven by the role and/or user selected. The user clicks Verify Selection After the user selects role, user, time and location parameters for all the fields.

Step 4: The entered information is verified for consistency in this step. The generic liveness and safety properties are defined before hand and are stored in a database. The form of these properties is depicted in Table 1. This step will evaluate the safety and liveness properties and in case of any violations, the user will be presented the correct webpage to make changes.

Step 5: The verified ODRs are stored in the ODR base to be used by Method 3 for composition of the disclosure rules.

Method 3: Composition and verification of disclosure rules based on ODRs, ARs, CPs and User Intentions (UIs).

Method 3 relates to disclosure rule composition and verification by the user. The proposed step-wise composition and verification method is outlined next (for overall context refer to Fig. 7).

Generally, the user selects disclosure intentions at each step of the composition process, prompting the system to verify the new intentions and suggest possible next steps. This method also allows reviewing partially composed as well as finalized rules with an option to retract previous rule composition steps. At all times the previous states of the rules, as well as the next possible steps are presented to the user visually in a user-friendly manner. The aim in this regard is to be able to capture the intentions of the user while at the same time presenting viable rule alternatives for the next step in disclosure rule composition. The underlying formalism is a Finite State Machine (FSM) based path transversal where each state leads to a set of states, some out of which may be viable, while others may not be viable. The method guides a user to the viable paths that can be followed.

The process involved in Method 3 is depicted in Fig. 12. Next, we provide details of each step of the process.

Step 1: In this step the user selects data elements to share with *consumers*. The selection of data elements can be done at a general level (e.g. all radiology data) or at a specific level (by selecting a specific data element). This list of data elements is based on all data (related to the user) uploaded by all *contributors* of data. Fig. 13 depicts a screen shot of this step.

Step 2: This step allows the user to select *consumers* to whom selected data can be released. The list of *consumers* in this case is based on the ODRs defined by the *contributor*. In case the ODRs do not limit disclosure to any *consumer*, a complete list of *consumers* defined for the user (in ARs) is presented. This step is depicted in Fig. 14.

Step 3: In this step the user selects the location of access for the selected *consumer* to access the selected data element. The list of locations is also entered by the *consumer* at the time of composition of ARs. This step is depicted in Fig. 15.

Step 4: The user selects the time of access in this step. The listed times are the ones entered by the consumer while composing ARs. Note, the location-time pair has already been verified as part of method 1. This step is depicted in Fig. 16.

Step 5: This step allows the user to review all selections and change any, if necessary. Note that change of any of the selected options is available to the user at all times. In case no change is required, the rule is saved in the DRB. A screen shot of this step is depicted in Fig. 17.

Method 4: Enforcement of disclosure rules on access of data from the UDR based on context of request.

Method 4 involves the enforcement of disclosure rules on the data requested by the user (for overall context refer to Fig. 7). The enforcement decision depends on the context parameters extracted from the request as well as from context sensors (such as system clock, in case of time). The process to implement Method 4 is depicted in Fig. 18.

Step 1: The request submitted by the *consumer* contains context parameters such as IP address or GPS reported location, user credentials etc. These parameters are extracted in this step.

Step 2: Additional context parameters may also be extracted using sensors in the system, such as time of day etc. The system clock is the sensor in this case.

Step 3: The disclosure rules held in the DRB are retrieved in this step and are compared with the context parameters collected as part of Step 1 and 2. The decision to whether or not return data to the *consumer* is also taken at this step.

Step 4: Relevant data is retrieved from the data store in the UDR. This data conforms to the privacy intentions defined in the disclosure rules by the user under the current context information.

Step 5: The relevant data is sent back to the *consumer*. In case there is no data to be sent back (disclosure rules do not allow), then a relevant error message along with complete details of the decision process is sent back to the *consumer*.

Method 5: Extraction of ARs from Question and Answer (Q&A) session between *Owner* and *Consumer*

Method 5 is an optional method meant for the *owner* and *consumer* to interactively compose ARs. At times this method may also be used to resolve conflicts in the ARs. The process to implement Method 5 is depicted in Fig. 19. We describe each step in detail below.

Step 1: The *owner* and the *consumer* initiate a question and answer session in free text format. In this session the *owner* may ask the *consumer* questions related to his or her credentials and clarify previously entered ARs. The Q&A session may be in real-time (both *owner* and *consumer* online at the same time) or can be such that the *owner* can leave a message for the *consumer*, who in turn replies when he comes online.

Step 2: This step involves the extraction of access rules from the contents of the Q&A session. In this regard the *owner* is presented with the likely rules extracted automatically from the session and is asked to validate them. Once the rules are validated they are stored in the AR base.

What is claimed is:

1. An intelligent system for defining context-aware disclosure rules for information stored in an online database, comprising:

   a. an intelligent context-aware disclosure rule composition module,

   b. an originator disclosure rule composer module,

   c. an access rule composer module,

   d. an enforcement module, and

   e. a free format text Question and Answer based rule composer.

2. The system of claim 1, wherein the user, the *owner* of the information defines disclosure rules by utilizing the intelligent feedback from the system based on runtime verification of composed rules.

3. The system of claim 1, wherein a contributor defines context-aware originator disclosure rules and contributes data to the system

4. The system of claim 1, wherein a consumer of information defines context-aware access rules governing all access to information held by the system.

5. The system of claim 1, wherein the enforcement module applies disclosure rules to the requested information.

6. The system of claim 1, wherein the rules are stored in a database.

7. The system of claim 1, wherein the system is an online repository of information of which the user is the *owner*.

8. The system of claim 1, wherein the system enables the user to define context-aware disclosure rules for information that may be privileged and cannot be released to the public.

9. The system of claim 1, wherein the system allows the user to define disclosure rules based on the context of the user, originator or consumer of information.

10. The system of claim 1, wherein the system allows the user to interact with the consumer (both in real-time as well as offline) and interactively compose access rules, which are then used for the composition of disclosure rules.

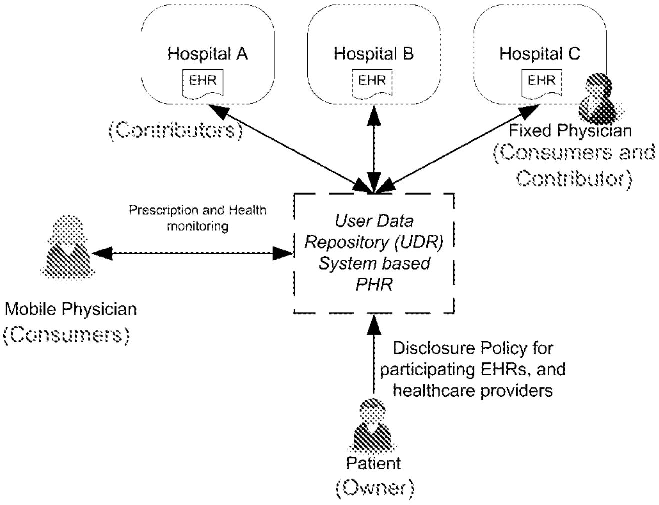

Hospital A
EHR
Hospital B
EHR
Hospital C
EHR
(Contributors)
Fixed Physician
(Consumers and Contributor)
Prescription and Health monitoring
User Data Repository (UDR) System based PHR
Mobile Physician
(Consumers)
Disclosure Policy for participating EHRs, and healthcare providers
Patient
(Owner)

Fig. 1

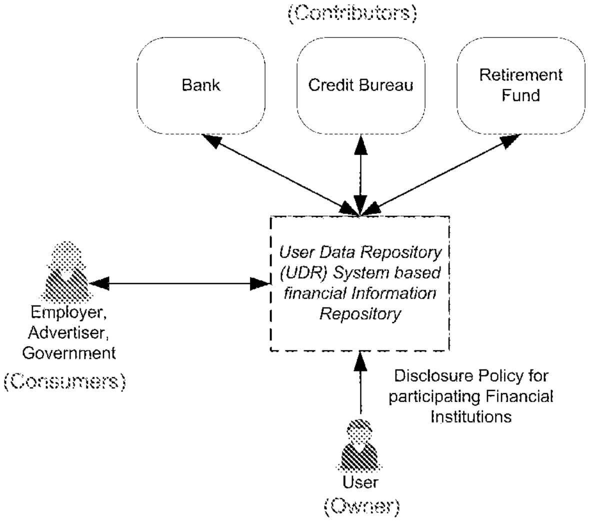

(Contributors)
Bank
Credit Bureau
Retirement Fund
User Data Repository (UDR) System based financial Information Repository
Employer, Advertiser, Government
(Consumers)
Disclosure Policy for participating Financial Institutions
User
(Owner)

Fig. 2

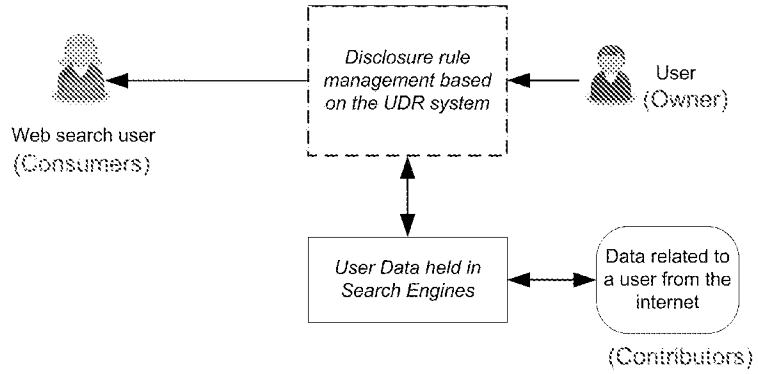

Disclosure rule management based on the UDR system
User (Owner)
Web search user (Consumers)
User Data held in Search Engines
Data related to a user from the internet
(Contributors)

Fig. 3

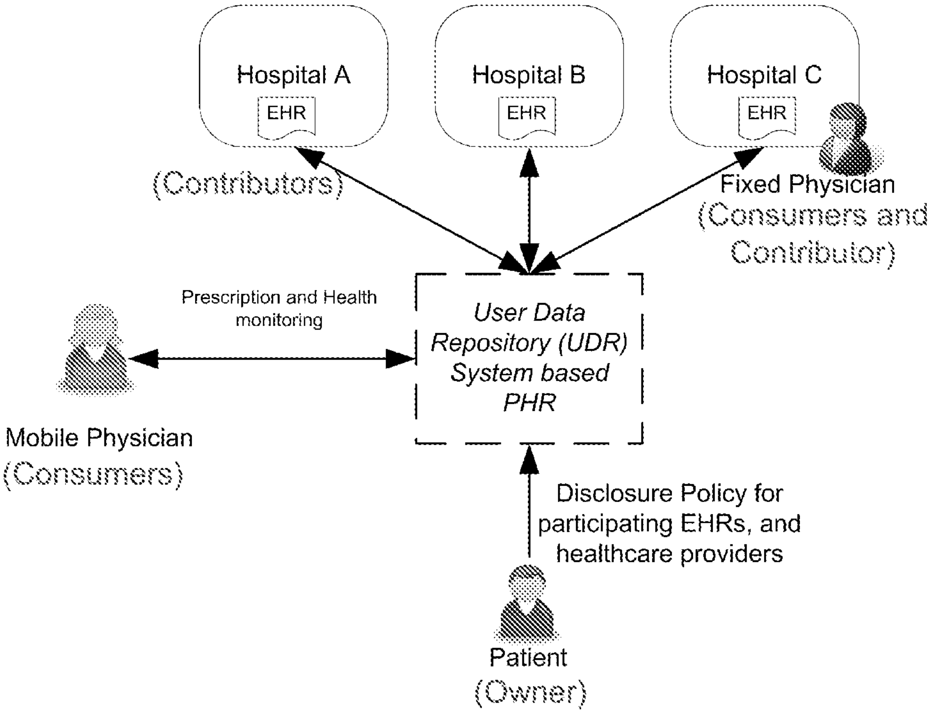

Hospital A
EHR
Hospital B
EHR
Hospital C
EHR
(Contributors)
Fixed Physician (Consumers and Contributor)
Prescription and Health monitoring
User Data Repository (UDR) System based PHR
Mobile Physician (Consumers)
Disclosure Policy for participating EHRs, and healthcare providers
Patient (Owner)

Fig. 4

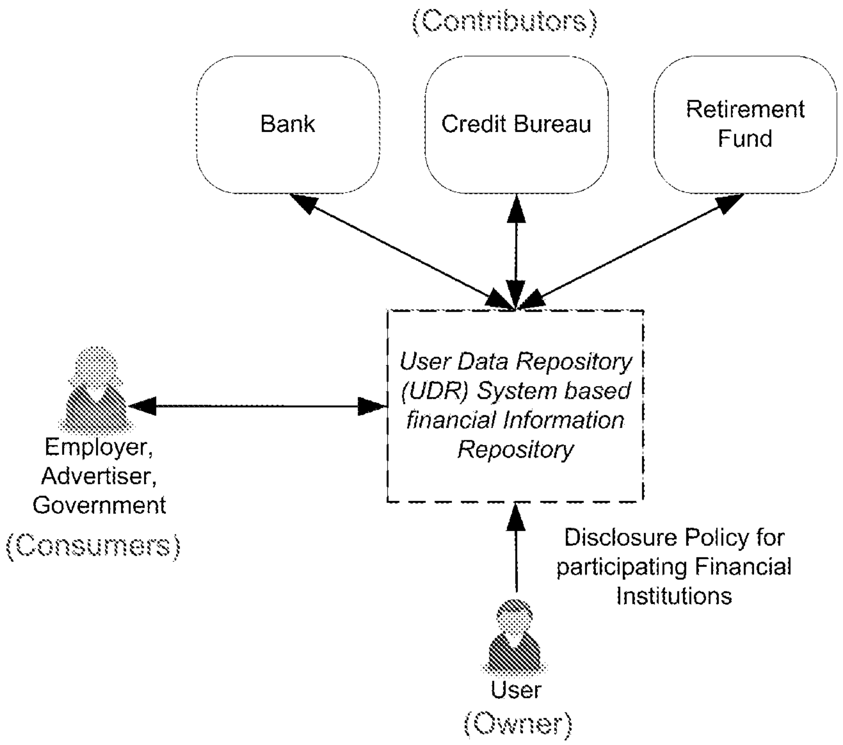

(Contributors)
Bank
Credit Bureau
Retirement Fund
User Data Repository (UDR) System based financial Information Repository
Employer, Advertiser, Government
(Consumers)
Disclosure Policy for participating Financial Institutions
User
(Owner)

Fig. 5

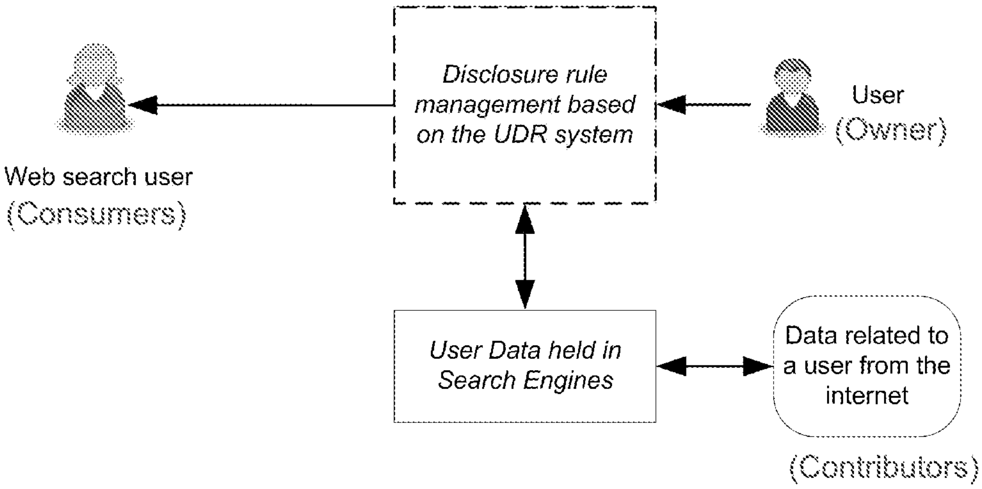

Disclosure rule management based on the UDR system
User
(Owner)
Web search user
(Consumers)
User Data held in Search Engines
Data related to a user from the internet
(Contributors)

Fig. 6

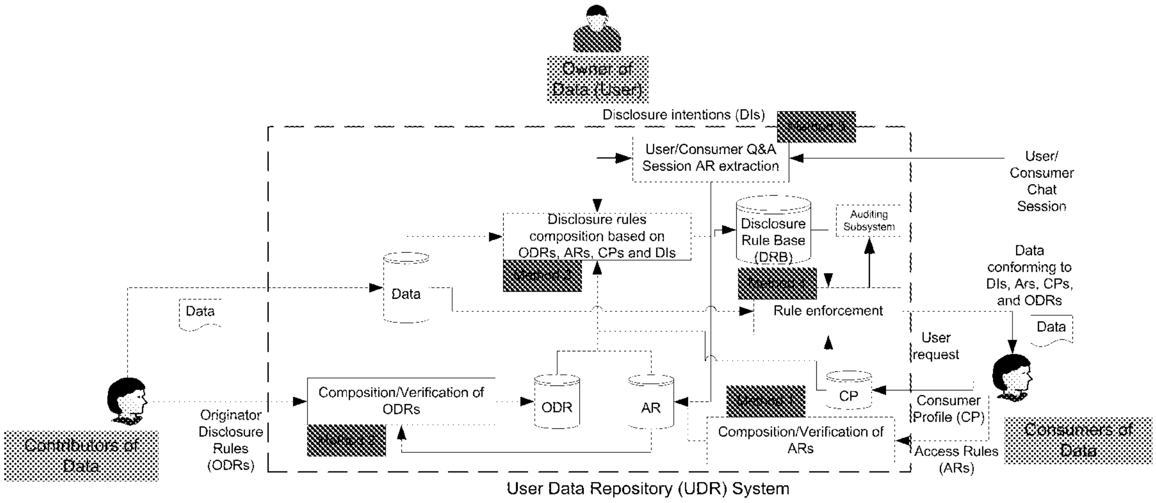

Owner of Data (User)
Disclosure intentions (DIs)
Method 3
User/Consumer Q&A Session AR extraction
User/ Consumer Chat Session
Disclosure rules composition based on ODRs, ARs, CPs and DIs
Method 2
Disclosure Rule Base (DRB)
Auditing Subsystem
Method 4
Data
Data
Rule enforcement
Data conforming to DIs, Ars, CPs, and ODRs
Data
User request
CP
Consumer Profile (CP)
Composition/Verification of ODRs
ODR
AR
Method 1
Composition/Verification of ARs
Access Rules (ARs)
Method 2
Originator Disclosure Rules (ODRs)
Contributors of Data
Consumers of Data
User Data Repository (UDR) System

Fig. 7

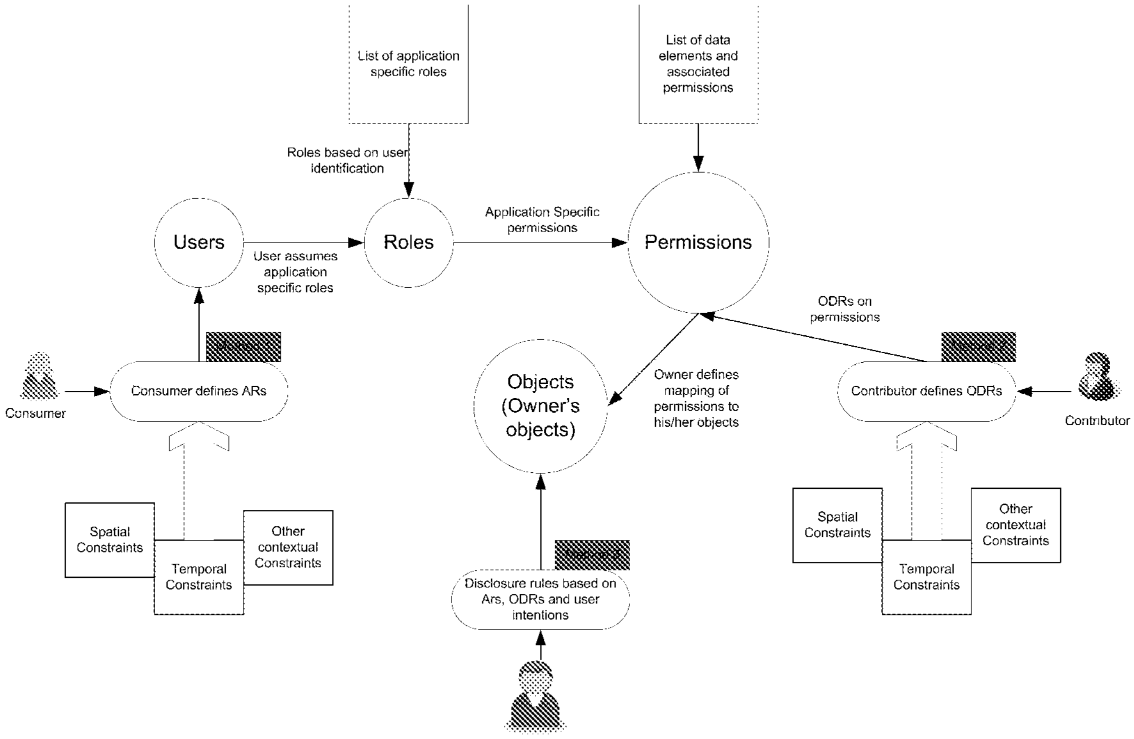

List of application specific roles
List of data elements and associated permissions
Roles based on user identification
Users
User assumes application specific roles
Roles
Application Specific permissions
Permissions
ODRs on permissions
Consumer
Consumer defines ARs
Objects (Owner's objects)
Owner defines mapping of permissions to his/her objects
Contributor defines ODRs
Contributor
Spatial Constraints
Temporal Constraints
Other contextual Constraints
Disclosure rules based on Ars, ODRs and user intentions
Spatial Constraints
Temporal Constraints
Other contextual Constraints

Fig. 8

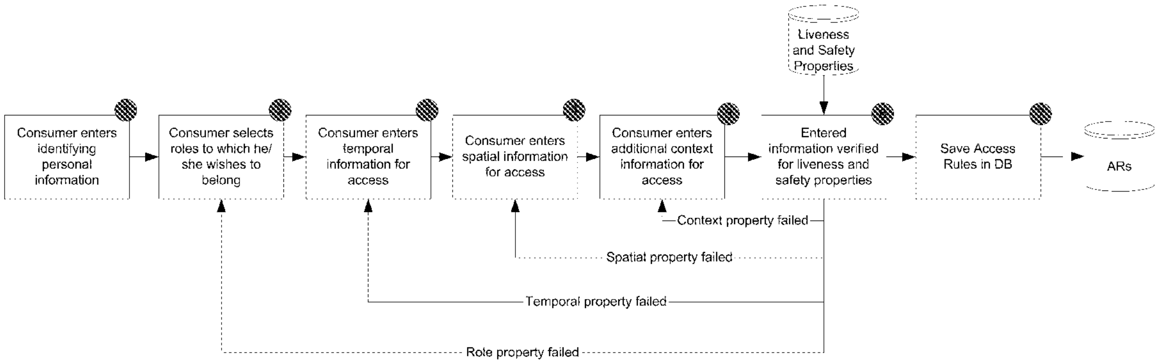

Liveness and Safety Properties
Consumer enters identifying personal information
Consumer selects roles to which he/ she wishes to belong
Consumer enters temporal information for access
Consumer enters spatial information for access
Consumer enters additional context information for access
Entered information verified for liveness and safety properties
Save Access Rules in DB
ARs
Context property failed
Spatial property failed
Temporal property failed
Role property failed

Fig. 9

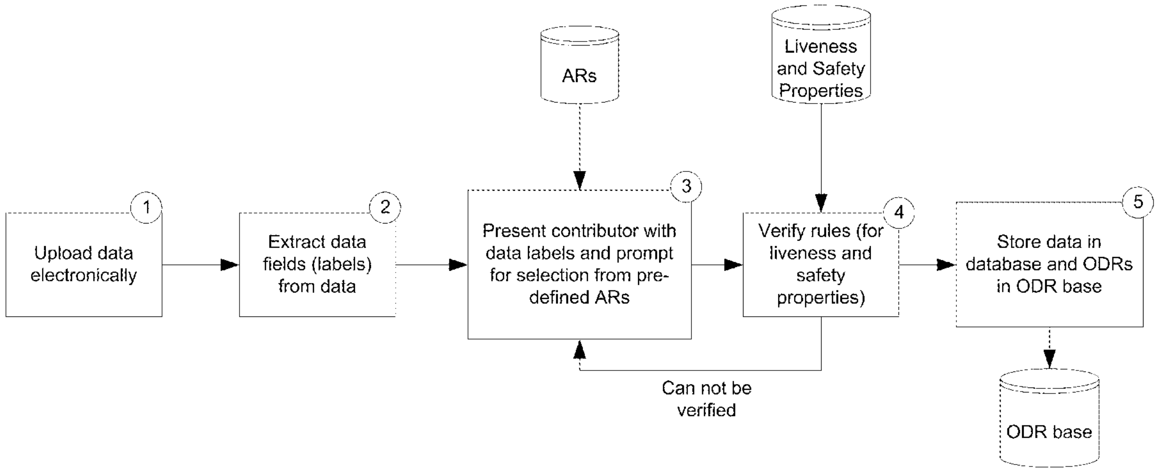
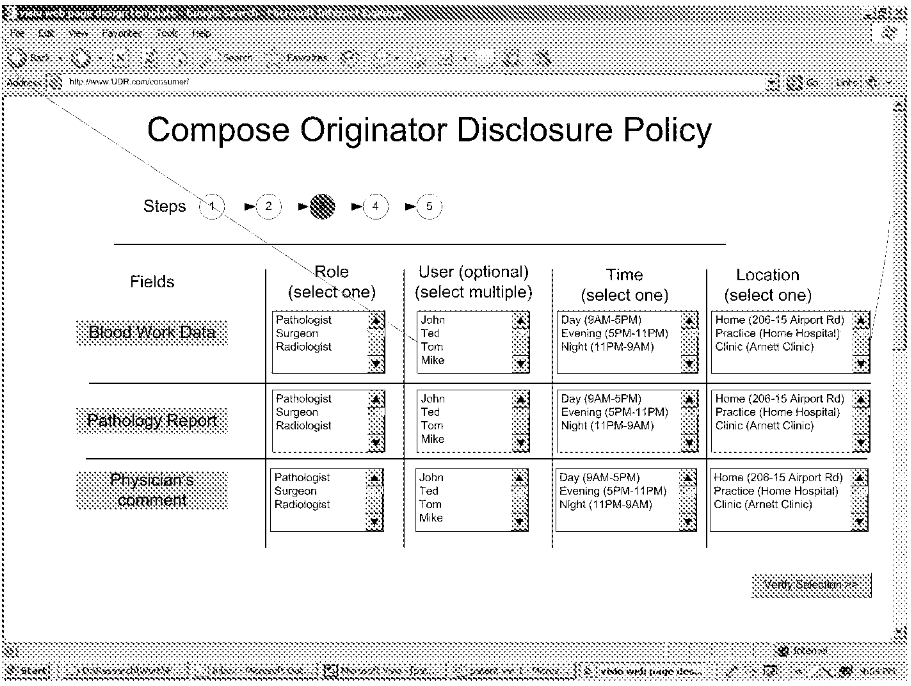

ARs
Liveness and Safety Properties
1
Upload data electronically
2
Extract data fields (labels) from data
3
Present contributor with data labels and prompt for selection from pre-defined ARs
4
Verify rules (for liveness and safety properties)
5
Store data in database and ODRs in ODR base
Can not be verified
ODR base

Fig. 10

Usernames updated for the selected role



Compose Originator Disclosure Policy

Steps 1 ► 2 ► ● ► 4 ► 5

Fields	Role (select one)	User (optional) (select multiple)	Time (select one)	Location (select one)
Blood Work Data	Pathologist Surgeon Radiologist	John Ted Tom Mike	Day (9AM-5PM) Evening (5PM-11PM) Night (11PM-9AM)	Home (206-15 Airport Rd) Practice (Home Hospital) Clinic (Arnett Clinic)
Pathology Report	Pathologist Surgeon Radiologist	John Ted Tom Mike	Day (9AM-5PM) Evening (5PM-11PM) Night (11PM-9AM)	Home (206-15 Airport Rd) Practice (Home Hospital) Clinic (Arnett Clinic)
Physician's comment	Pathologist Surgeon Radiologist	John Ted Tom Mike	Day (9AM-5PM) Evening (5PM-11PM) Night (11PM-9AM)	Home (206-15 Airport Rd) Practice (Home Hospital) Clinic (Arnett Clinic)

Time and location updated for the selected role

Fig. 11

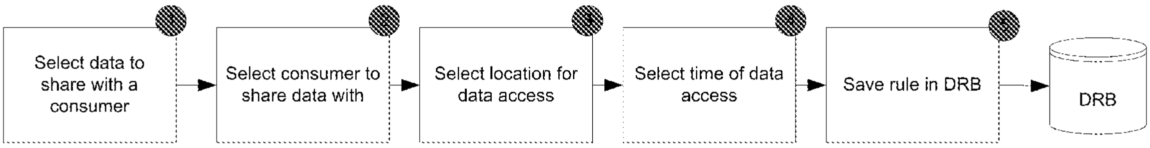
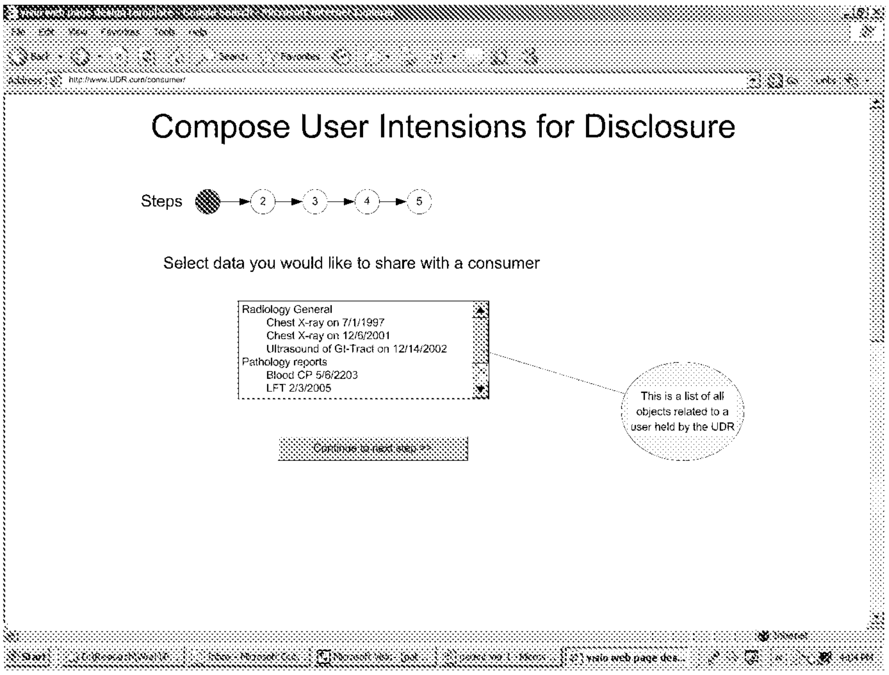

Select data to share with a consumer
Select consumer to share data with
Select location for data access
Select time of data access
Save rule in DRB
DRB

Fig. 12



Compose User Intensions for Disclosure

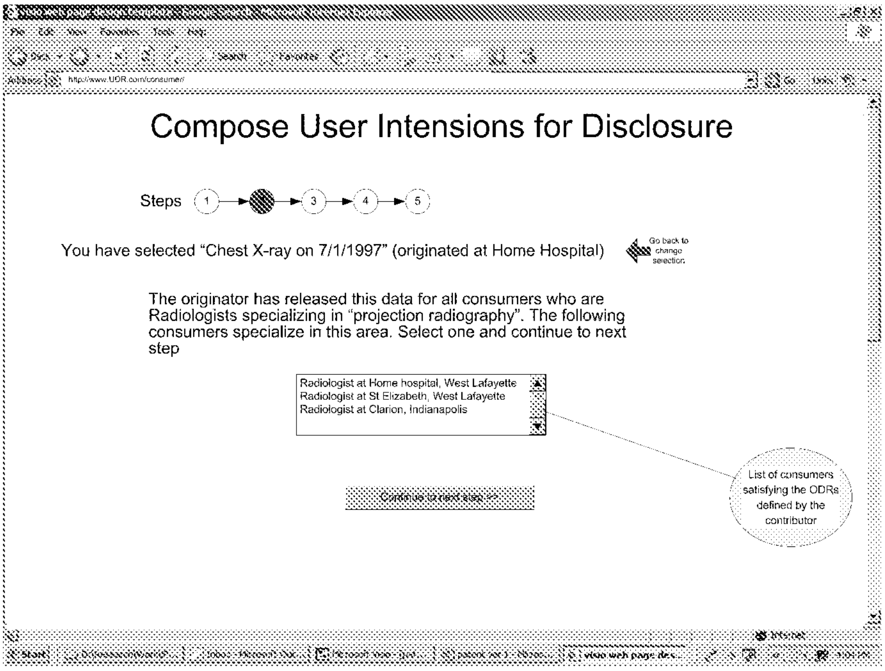
Steps ● → 2 → 3 → 4 → 5

Select data you would like to share with a consumer

Radiology General
Chest X-ray on 7/1/1997
Chest X-ray on 12/6/2001
Ultrasound of GI-Tract on 12/14/2002
Pathology reports
Blood CP 5/6/2203
LFT 2/3/2005

http://www.UDR.com/consumer/
Continue to next step >>
This is a list of all objects related to a user held by the UDR

Fig. 13



Compose User Intensions for Disclosure

Steps 1 → ● → 3 → 4 → 5

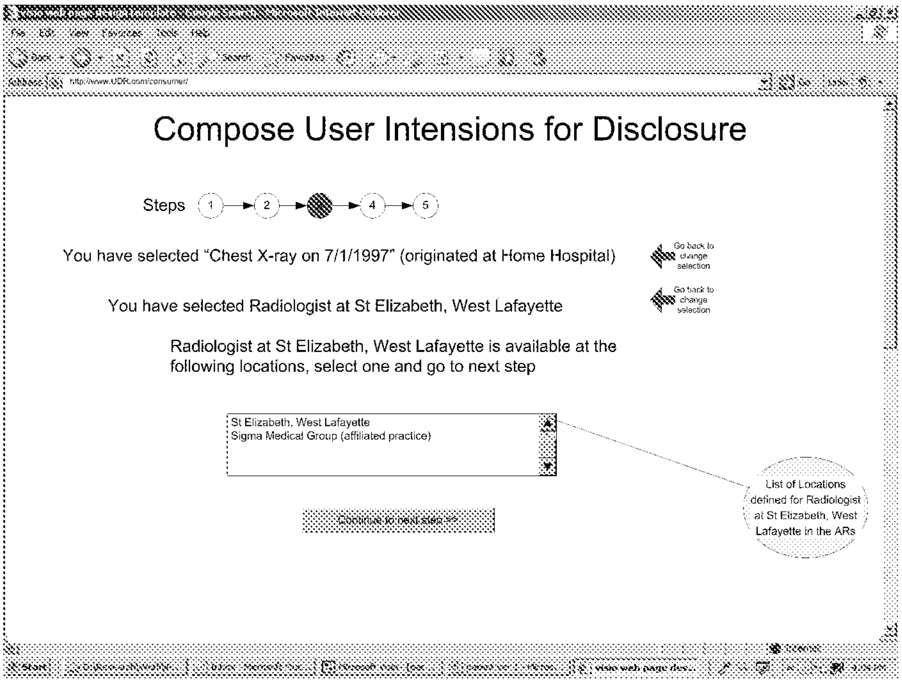
You have selected “Chest X-ray on 7/1/1997” (originated at Home Hospital)

The originator has released this data for all consumers who are Radiologists specializing in “projection radiography”. The following consumers specialize in this area. Select one and continue to next step

Radiologist at Home hospital, West Lafayette
Radiologist at St Elizabeth, West Lafayette
Radiologist at Clarion, Indianapolis

http://www.UDR.com/consumer/
Go back to change selection
Continue to next step >>
List of consumers satisfying the ODRs defined by the contributor

Fig. 14


http://www.UDR.com/consumer/
Steps 1 2 4 5
Go back to change selection
Go back to change selection
Continue to next step >>
List of Locations defined for Radiologist at St Elizabeth, West Lafayette in the ARs

Compose User Intensions for Disclosure

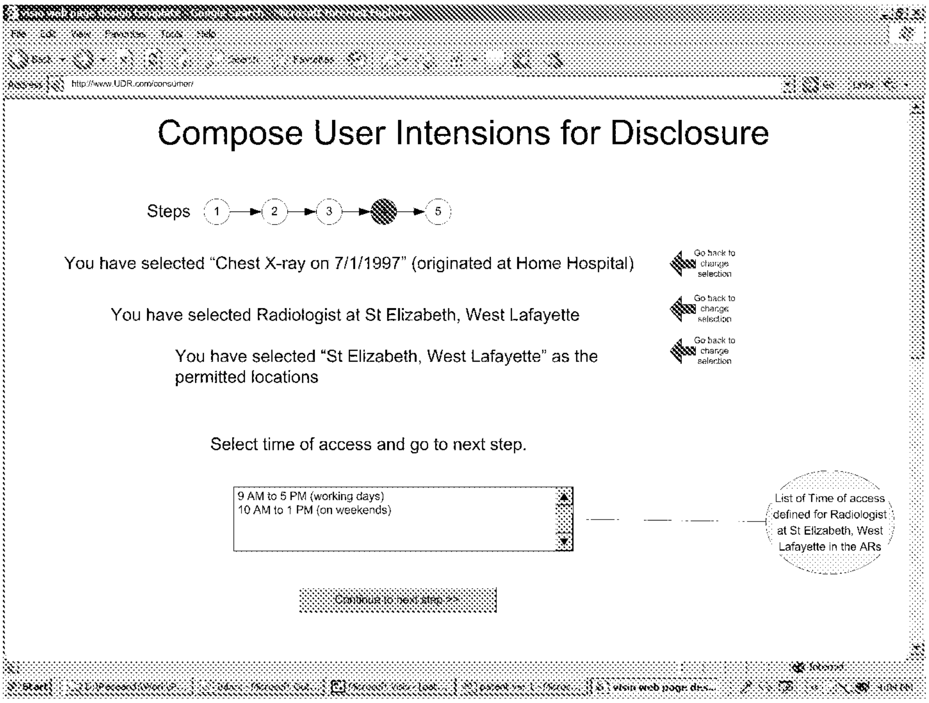
You have selected “Chest X-ray on 7/1/1997” (originated at Home Hospital)

You have selected Radiologist at St Elizabeth, West Lafayette

Radiologist at St Elizabeth, West Lafayette is available at the following locations, select one and go to next step

St Elizabeth, West Lafayette
Sigma Medical Group (affiliated practice)

Fig. 15


http://www.UDR.com/consumer/
Steps 1 2 3 5
Go back to change selection
Go back to change selection
Go back to change selection
Continue to next step >>
List of Time of access defined for Radiologist at St Elizabeth, West Lafayette in the ARs

Compose User Intensions for Disclosure

You have selected “Chest X-ray on 7/1/1997” (originated at Home Hospital)

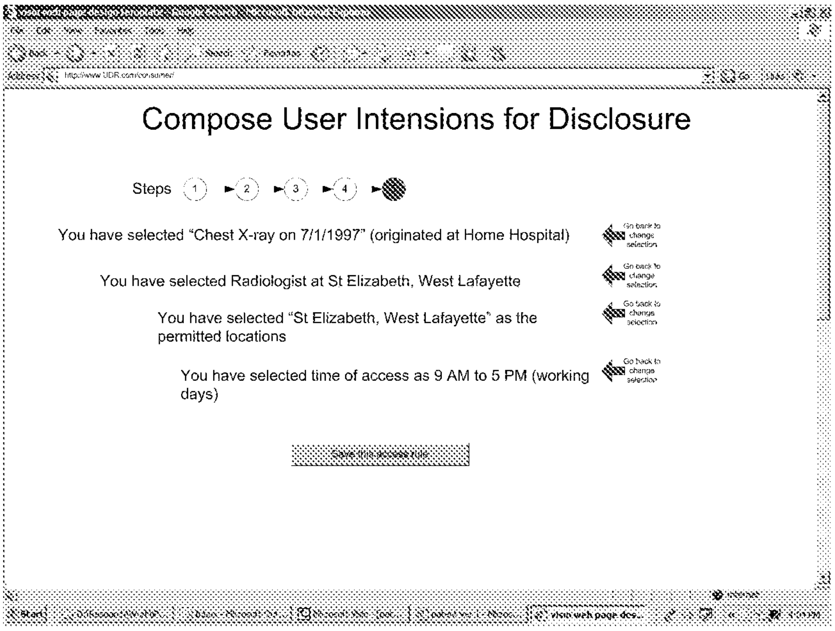
You have selected Radiologist at St Elizabeth, West Lafayette

You have selected “St Elizabeth, West Lafayette” as the permitted locations

Select time of access and go to next step.

9 AM to 5 PM (working days)
10 AM to 1 PM (on weekends)

Fig. 16



http://www.UDR.com/consumer/

Compose User Intensions for Disclosure

Steps 1 ► 2 ► 3 ► 4 ► ●

You have selected "Chest X-ray on 7/1/1997" (originated at Home Hospital)

Go back to change selection

You have selected Radiologist at St Elizabeth, West Lafayette

Go back to change selection

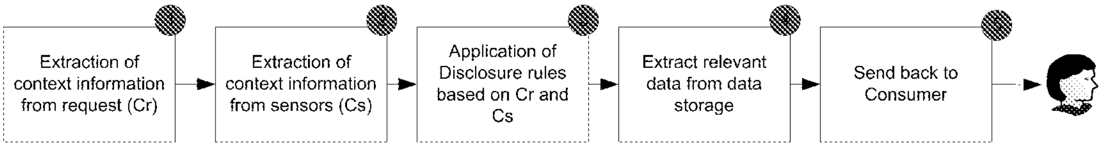
You have selected "St Elizabeth, West Lafayette" as the permitted locations

Go back to change selection

You have selected time of access as 9 AM to 5 PM (working days)

Go back to change selection
Save this access rule

Fig. 17



Extraction of context information from request (Cr)
Extraction of context information from sensors (Cs)
Application of Disclosure rules based on Cr and Cs
Extract relevant data from data storage
Send back to Consumer

Fig. 18

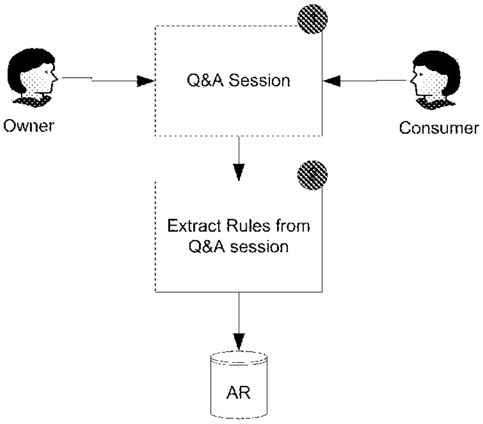


Fig. 19

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 08/78866

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 15/16 (2008.04)
USPC - 707/1
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)
USPC: 707/1

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 707/1, 2, 9, 10; 726/1, 2, 3, 27 (text search -- see terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST(USPT, PGPB, EPAB, JPAB); DialogPRO; Google
Search Terms: Information, secure, securing, access, online, store, database, internet, repository, privilege, non-public, Rules, compose, composition, disclosure, context- aware, define, standard, module, originator, enforce, free-form, text, question,answer etc.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 6,314,409 B2 (SCHNECK et al.) 06 November 2001 (06.11.2001), FIG. 1, 2, 3, and 5, col 7, ln 15-48; col 10, ln 26-31, 47-60; col 11, ln 4-15; and col 15, ln 31-40	1 and 3-9 ------------ 2 and 10
Y	US 7,233,948 B1 (SHAMOON et al.) 19 June 2007 (19.06.2007), FIG. 1 and 11, and col 15, ln 18-26, 53-57	2
Y	US 6,658,400 B2 (PERELL et al.) 02 December 2003 (02.12.2003), FIG. 8B, col 1, ln 9-17; and col 25, ln 21-30	10

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

* 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
25 November 2008 (25.11.2008)

Date of mailing of the international search report
11 DEC 2008

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-3201

Authorized officer:
Lee W. Young
PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774