

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

(19) World Intellectual Property Organization

International Bureau



(10) International Publication Number

WO 2013/030260 A1

(43) International Publication Date

7 March 2013 (07.03.2013)

(51) International Patent Classification:

H04L 29/06 (2006.01) G06F 21/00 (2013.01)

(21) International Application Number:

PCT/EP2012/066837

(22) International Filing Date:

30 August 2012 (30.08.2012)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/530,416 2 September 2011 (02.09.2011) US
11191213.5 29 November 2011 (29.11.2011) EP

(71) Applicant (for all designated States except US): NAGRA-VISION S.A. [CH/CH]; Route de Genève 22-24, CH-1033 Cheseaux-sur-Lausanne (CH).

(72) Inventor; and

(75) Inventor/Applicant (for US only): NICOLAS, Christophe [CH/CH]; Chemin de Sous-Allens 15, CH-1162 Saint-Prex (CH).

(74) Agent: WENGER, J.; Leman Consulting S.A., Chemin de Précossy 31, CH-1260 Nyon (CH).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, 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, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- with amended claims (Art. 19(1))

(54) Title: METHOD TO CONTROL THE ACCESS OF PERSONAL DATA OF A USER

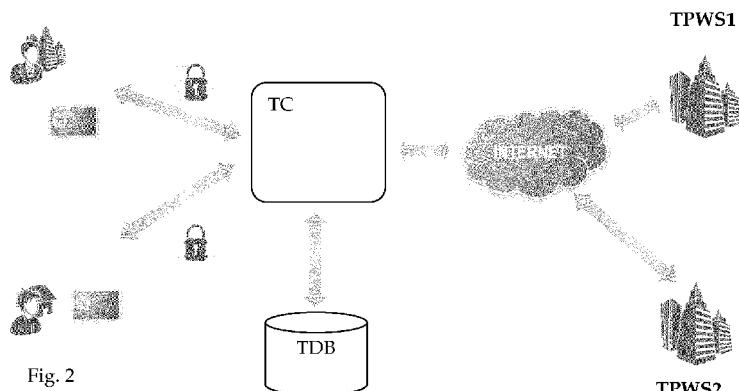


Fig. 2

(57) **Abstract:** There is a need for a system and method that is designed to give full and continued control of his data by a user, gain the trust of the average individual, encouraging such individual to become an open-minded and trustful user of such system. It is proposed a method to control the access of personal data of a user by a trusted centre comprising at least one database comprising for a specific user, memory locations for personal data, access conditions associated to the personal data and management data comprising at least a counter, - loading by a user into the database of the trusted center, its personal data and assigning access conditions to said data, said personal data being divided into at least two categories having two different access conditions, each category being associated with a user's value, - requesting access to the trusted centre by a third party to the personal data of a plurality of users, said request comprising search criteria, - executing by the trusted center the search criteria on the personal data of the users so as to determine a first set of users matching the search criteria, - returning to the third party information showing the quantity of the first set of users matching the criteria, as well as the sum of the user's value of each user of the first set, - acknowledging all of part of the sum by the third party, thus defining a second set of users that can comprise all or part of the first set, - returning the personal data of the second set of user for which the sum covers the accumulated values of the extracted users, - updating the counter of the second set of users with the content of the value of their respective personal data.

METHOD TO CONTROL THE ACCESS OF PERSONAL DATA OF A USER

Introduction

With the development of communication networks, users of these networks are increasingly solicited to give away personal data to service providers to feed such 5 personal data into data bases.

As the computerized environment increases in importance and performance, the average user is more and more frustrated by bad-quality computer engines that care too little about his privacy needs.

Background art

10 Some third parties put a high value on the personal data that an individual puts on various connected systems that are part of his everyday life. The use that such third parties can make goes from market studies to targeted advertising to data mining and the like.

So far, there has been no frame or structure to :

15 1) enable the user to keep full control of his personal data;
2) convince the user that he takes no disproportionate risk in giving away such data;
3) as a further possible step, formally monetize the personal data posted, thanks to the trust of the user, as direct benefit to said user.

20 The quality of data bases can be adversely affected by distrust of individuals. In the case of a census for instance, some free-thinking users adopt anti-establishment behaviors by providing false data, just because they do not trust the governmental entity that is requesting them to provide these data.

When the data provided is clearly out-of-range, cleaning the results flow is relatively 25 easy and can be done in an automated way, for example by simple cross-checks between responses provided by a single user. However, when the free-thinker is more sophisticated and knows how to outfox the automated checks, there is very little that can be done to obtain true data and a resulting good quality of aggregated data bases.

There is therefore a need for a system that is designed to give full and continued control of his data by a user, gain the trust of the average individual, encouraging such individual to become an open-minded and trustful user of such system.

The problem has become more acute with the increased popularity, especially 5 among young adults, of social networks. The managers of a number of such social networks tend have little consideration for any future disadvantages of the lack of experience of these young adults vis-à-vis the perception problems that a visitor of such social networks may encounter.

For example, a careless youngster can post on his personal storage, hosted by a 10 social network, some visuals that he, on second thought or years after, would rather restrict access to. Such visuals can be for instance videos or photographs shot during a private party, during which alcohol, or more generally substances able to modify the state of consciousness, were ingested or inhaled.

When said careless youngster becomes a graduate in search of a job, the fact that a 15 social network did grant access, by non-restricted or not enough restricted audiences, to clues of said way of life illustrated by the afore-mentioned visuals can be a disadvantage in finding a desired job.

If said youngster embraces a political career, the backlash can be even more severe, with evidence of a past life as a young man or woman being displayed by the press 20 to a large public, especially a senior or elderly public with little inclination to forgiveness, thus undermining the credibility of the person in question, even though that person may have grown up and regret his past behaviour as a youngster. The continued storing, in out-of-reach databases, of extracts of postings made by youngsters can thus become very detrimental to their professional or political future.

25 The problem is made more serious by the fact that the managers of social networks sometimes have a tendency to over-protect their organisation, should they become aware of data ownership issues, by altering the legal terms applying to the individual members of a given social network.

In such a case, a lack of consideration for the interests of such individual members 30 can result in severe damage to said interests. For instance, legal conditions are sometimes modified without notice, claiming ownership by the network of any and all data posted on the individual's personal storage.

Even if the information on such a change in legal terms is communicated to subscribers, there is a high probability that a vast majority of the younger users will not react and therefore implicitly accept such change. And even if some react and demand a deletion of the incriminated data, they face the perspective of a costly legal

5 action against said social network, with uncertain success. The cost to an individual of such legal action, as compared to the often disproportionate resources available to the social network as a defendant, can deter the individual from starting such action at all, entailing a sense of frustration on his part.

The number of cases where the credibility, or personal life, or professional future an

10 individual was undermined, or deteriorated, or compromised is on the rise, and so is the press coverage of such stories, as well as the resulting awareness of the public.

With the surge in this number of cases, a consequence of the afore-mentioned facts is an increased defiance vis-à-vis social networks in the public at large. However, the social networks are trendy and gaining momentum among the younger public. This

15 makes them unavoidable to a large extent to ambitious personalities, who do not always realize the danger they represent for their future social life.

Brief description of the invention

It is proposed a method to control the access of personal data of a user by a trusted centre comprising at least one database comprising for a specific user, memory

20 locations for personal data, access conditions associated to the personal data and management data comprising at least a counter,

- loading by a user into the database of the trusted center, its personal data and assigning access conditions to said data, said personal data being divided into at least two categories having two different access conditions, each category being

25 associated with a user's value,

- requesting access to the trusted centre by a third party to the personal data of a plurality of users, said request comprising search criteria,

- executing by the trusted center the search criteria on the personal data of the users so as to determine a first set of users matching the search criteria,

- returning to the third party information showing the quantity of the first set of users matching the criteria, as well as the sum of the user's value of each user of the first set,
- acknowledging all of part of the sum by the third party, thus defining a second set of users that can comprise all or part of the first set,
- returning the personal data of the second set of user for which the sum covers the accumulated values of the extracted users,
- updating the counter of the second set of users with the content of the value of their respective personal data.

10 ***Brief description of the drawing***

The present invention will be better understood thanks to the attached figures in which :

- the figure 1 shows a system with the trusted center connected to Internet
- the figure 2 shows a system in which the trusted center plays the role of a proxy.

15 ***Detailed description***

The invention consists in a subscription system to a trusted center TC open to at least one part of the general public, in which a subscribing member is encouraged, by defined system features, to keep full control of his personal data once they are fed onto the system. The subscribing member is therefore encouraged to provide true data to the trusted center.

Such defined trusted center TC features can consist in minimal standards of quality in processing said provided data. For instance, existing systems are able to track down the fact that an internet user has browsed sites of hotels in Italy, and immediately propose discounted-price travel offers to Italy to that user. Such offers can be perceived as intrusive and unwanted advertising. A minimum standard of quality can consist in defining, with each individual user, to what extent such automated offers can be generated and displayed.

Another defined system feature can also consist in providing the possibility to genuinely and reliably erase a history of data for the individual user.

In a particular embodiment of the invention, a system feature is designed to provide full transparency to a subscribing user.

In a particular embodiment of the invention, the system provides a differentiated level of control to a subscribing user, onto the type of data he feeds the system with.

5 As a first example, a first category of level of control is allocated to the user's preferences in sports. Such preference data can consist in his personal ratings in sports. For example, a user A can let the system know that he prefers basketball to football, football to tennis, and tennis to windsurfing. Such preference data can also consist in personal ratings on various competing teams in a given sport. As another 10 example, a user B may disclose, with a certain level of ownership and control, the information that he prefers a certain basketball team to another given basketball team.

As a second example, a second category or level of control is allocated to the user's hobbies.

15 As a third example, a second level of control is allocated to the user's political orientation. Data on political orientation may therefore be considered, by the user, as more sensitive than sports preferences or hobbies, and be granted a more restrictive level of protection against external, non-user access.

20 As a fourth example, a third level of control is allocated to the user's sexual preferences, orientation or habits.

As an additional example, a level of control is allocated to the user's investor's profile characteristics. Such characteristics can be financial conservativeness, risk-tolerance, inclination to alternate-scheme investments, fair-trade or nature conservation preferences in investment choices, or the like.

25 In a particular embodiment of the invention, the system provides a differentiated level of control on the different types of data as afore-mentioned.

This control can be exercised by different ways:

- a) directly through explicit choices,
- b) indirectly, for instance by defining access rules,
- 30 c) by proxy, i.e. by subcontracting a level of control to a trusted third party.

For each category, the user can define a user's value that represents the value of this information for said category. Different manner to fill this value can be applied.

- The user can freely define the value
- The system proposes predefined values, and the user select one

5 - The value is automatically added by the system and simply acknowledge by the user.

It is worth noting that the user can decide not to share a particular category of its personal data.

In fact, when a category matches the search criteria of the third party, it is not the category that is sent back to the third party but the user identification. For a given category, e.g. sport, the user can also decide which part of its identification is sent. He can select an e-mail address, a name, a location, a twitter or facebook account , i.e. information that can be used to allows the third party to propose services or goods to said user.

15 The method described above can be used in a more abstract level and in an anonymous way. The third party could be only interested to the number of hits for specific search criteria. For example, a company, before opening a sport shop in a specific place, can request the trusted center in order to obtain the number of people which are sport regular in a geographic zone close to the future shop. In this case, 20 the trusted center does not send back the identification of the user.

For this case, each category of the personal data can have in fact two user's values, one for having access to the user's identification and another one for simply participating to this anonymous search.

25 The result of the search can give a large number of hits. This is why the present method proposes some optimization features. In the case that the user's value can have different content, i.e. for one user, 0.1 cent and another user, 0.2 cent, the trusted center will organize the data transmitted to the third party by grouping the users having the same amount. The trusted center presents the information by amount, e.g. 1200 users at 0.1 cent and 2300 users at 0.2 cent (of the users 30 satisfying the search criteria). The third party can then decide to refine the search by

adding additional search criteria and rerun the request to the trusted center or can accept the deal proposed for the first set of user.

In the search criteria sent by the third party, the latter can include a limit value. This value will define how many hits will be returned to the third party by the trusted 5 center. This limit value corresponds to the accrued user's value until the limit value is reached.

It is well known that the interest for the personal data is higher if they are accurate. This is why the trusted center can carry out various verifications on the personal data with or without the help of the user. The user can have an interest that his data are 10 validated, thus allowing a higher value for each of the category. The verification will focus on the age, gender, address and other personal data. It is more difficult to verify the preferences such as preferred color, vacation destination etc.

When the user profile is verified by the trusted center the trusted center can increase the user's value. The third party can also include in the search criteria the possibility 15 to access only validated user (and usually pay more) or all user's.

In the figure 2, the embodiment illustrates the case where the trusted center TC plays the role of a proxy. The various users UT1, UT2 first connect to the trusted center TC and from this center, have access to the third party websites TPWS1, TPWS2. In this case, the user first connects through the trusted center TC to a third party website 20 TPWS. At that time, the functionality of the TC could be transparent and the identification and authentication of the user will take place at a later stage.

In another embodiment, the proxy authenticates the user prior to accessing the TPWS.

The TPWS then request the identification of the user and this request is passed to 25 the TC. The latter can check if the personal data (all or part) of the user are accessible to this TPWS. In the positive event, the personal data are sent back to the TPWS. Beside that, the user can be identified by a unique identifier for said TPWS, this identifier being the same each time the user connects to the TPWS but unique to said TPWS.

30 In a particular embodiment of the invention, the system provides a differentiated level of control on the data via different encryption features applied on the data.

According to a first way of implementing the invention, the user, via its user's terminal UT, connects to a trusted centre TC and loads its personal data, thanks to a secure communication between the user and the trusted centre.

As explained above, the personal data are divided into categories and each category

5 is assigned to particular access right. In the access right, several data can be defined such as the third party allowed accessing these data. This setting can be in the form of a list of third party websites (e.g. Facebook™, Twitter™, LinkedIn™) that the user sticks if the data of this category is accessible to this third party website. The personal data could also be pictures, texts of movies.

10 Beside that, it is possible to define rules for exploiting the personal data such as defining financial compensation in case the personal data are transferred to a third party. For each category of personal data, a particular amount can be defined.

The third party web service TPWS can also enroll into the trusted database TDB. A profile can be defined as well as a description of the type of activity (e.g. sport

15 activities, information). This third party can define the type of users it is interested to such as young male or person with pets.

This web service can also define the compensation for accessing user's personal data matching the categories of interest by this web service, this compensation could be associated to the entire user's record or split by user's data category.

20 In a second step, the user accesses a third party website TPWS and is invited to identify himself. In order to obtain the personal data by the third party website, the latter initiates a secure link with the trusted centre and transmits the identity of the user as well as an identifier of the third party website.

The trusted center will then authenticate the user through this link and will request

25 the credential of the user. This can be in the form of a password or based on a more secure operation involving a one time password (using a personal card that generates this one time password). Once the user has been authenticated, the trusted center checks the access conditions to the personal data using the identifier of the third party website. In view of this verification, the personal data are (or aren't) 30 returned to the third party website.

The request to the trusted center can also include filter information. The third party website can be interested to only a part of the personal data (by using the descriptor

of the data) or can also limit the type of the size of the data. In case that the personal data comprises a movie of 500 Mbytes, the third party website can specify the maximal size of the data requested. Instead or in addition to the size, the third party website can specify the type of data he is interested on, e.g. preferences, pictures etc.

To identify the user, the third party can receive a unique identifier from the trusted center, this identifier identifying the user on one hand but being unique for the third party on the other hand. In this case, the third party receives the personal data of the user currently accessing its services without knowing the true identity of the user.

10 During the authentication process, the third party can also add some category(ies) of interest and transmit it to the trusted centre. The latter can then verify if the user currently authenticated matches the category identified by the third party and in the positive event, the personal data of the user can be transmitted to the third party. In case that a financial compensation was defined by the user, and accepted by the

15 third party, a credit is made on the user's account, credit provided by the third party. The user's counter will then be incremented.

As explained above, the trusted center can play the role of the proxy. The trusted center database contains the personal data and the proxy first identifies the user. Once identified, the trusted center can oversee the communication between the

20 user's terminal and a website. In case that the user has blocked some personal data, such as the telephone number, the trusted center can warn the user in case the telephone number is requested. For the proxy mode, the goal is to catch personal data that would transit from the user to the website. It is hard to block a site that would request personal data but it is easy to block data that we know (i.e. the data given by the user to the trusted center). In this mode the proxy acts as a DLP (Data Loss Prevention) device.

25 In a lighter version, it is possible to load a small software application into the user's computer to store its user's identification for the trusted center. When the user accesses to a third party web service, having itself an account with the trusted centre, the user can authorize to access its personal data to this third party (generally against compensation). This authorization can be in the form of clicking into a logo of the trusted center in the third party webpage. In order to keep the anonymity of the

user, the third party transmits to the user's application an identifier (IDTP) of the third party. The user's application stores the user's identifier (IDU), a personal key (KUp), the private key of an asymmetric key pair, and a trusted center key (KTpu), the public key of the trusted center.

5 The user's application generates two cryptograms, the first cryptogram $(IDU)_{KTpu}$ is obtained by the encryption of the user's identifier IDU with the trusted center key KTpu and the second cryptogram $(IDTP)_{KUp}$ is obtained by the encryption of the third party identifier IDTP by the personal key KUp. It is to be noted that the second cryptogram represents for the third party a unique identifier that allow to check if this

10 user has already visited this third party. In the positive event, the data collected during previous visit, as well as possible personal data of this user can be used to personalize the presentation of the web offer.

In the case that the second cryptogram is new, it means that this user connects to the third party for the first time. The third party can access the trusted center and can

15 transmit the first cryptogram as well as its own identification. The trusted center can decrypt the first cryptogram in order to determine which user it concerns. The trusted center can return to the third party the personal data of said user in case that the user has authorized this transmission and the compensation rules are fulfilled.

Instead of asymmetric keys, the personal keys can be a symmetric secret key.

20 According to an embodiment of the invention, during the initialization of the personal data with the trusted center, or at a later stage, the user can receive cryptographic material in the form of an electronic certificate or a pair of asymmetric keys. This cryptographic material is stored on the user's device such as laptop, smartphone, tablet. This material is used during the authentication steps carried out by the third

25 party website. After the third party website has initiated the connection with the trusted center, the data exchanged between the user and the trusted center are encrypted using this cryptographic material. As a consequence, the third party website cannot interfere into the authentication procedure and cannot understand the data exchanged.

30 According to another embodiment, a third party website can send a request for obtaining personal data of users. In this request, this website can define its proposition in term of compensation for accessing the personal data as well as

search criteria. The trusted center will then search through its database to find the user's data that match the search criteria. Once a user has been found, the center verifies that the access conditions link to these data allow the transmission of these data. This verification can take into account the general access conditions such as if 5 this category is accessible to third party or if the third party is explicitly allowed to access these data.

In both cases, the user can define financial criteria to have access to his data and the trusted center compares the expectations of the user and the third party proposal. If a match is found, the user's personal data are transferred to the third party is credited 10 by the compensation offered by the third party.

In this particular embodiment of the invention, the system provides a possibility for the user to monetize the communication, under pre-defined conditions, of certain of his personal data to third parties that are ready to compensate him for such communication.

15 Such pre-defined conditions can include the permission to, or a denial of permission to, re-sell personal data, to third parties subject to afore-mentioned levels of control.

To implement the method of the invention, the trusted center has processing and storage capabilities as well as telecommunication means. The trusted center is preferably connected to Internet so that the users can post their personal data. The 20 processing capabilities are in charge of protecting the personal data, organizing them and carrying out the search requested by the third parties.

Claims :

1. Method to control the access of personal data of a user by a trusted centre comprising at least one database comprising for a specific user, memory locations for personal data, access conditions associated to the personal data and management data comprising at least a counter,
 - loading by a user into the database of the trusted center, its personal data and assigning access conditions to said data, said personal data being divided into at least two categories having two different access conditions, each category being associated with a user's value,
- 5 - requesting access to the trusted centre by a third party to the personal data of a plurality of users, said request comprising search criteria,
- 10 - executing by the trusted center the search criteria on the personal data of the users so as to determine a first set of users matching the search criteria,
- 15 - returning to the third party information showing the quantity of the first set of users matching the criteria, as well as the sum of the user's value of each user of the first set,
- 20 - acknowledging all of part of the sum by the third party, thus defining a second set of users that can comprise all or part of the first set,
- 25 - returning the personal data of the second set of user for which the sum covers the accumulated values of the extracted users,
- 30 - updating the counter of the second set of users with the content of the value of their respective personal data.

2. The method of claim 1, wherein the information showing the quantity of the first set of users matching the criteria comprises the steps of :
 - grouping all users of the first of users that have the same user's value,
 - transmitting to the third party, the quantity of user per group.
3. Method to control the access of personal data of a user by a trusted centre comprising at least one database comprising for a specific user, memory locations for personal data, access conditions associated to the personal data and management data comprising at least a counter,

- loading by a user into the database of the trusted center, its personal data and assigning access conditions to said data, said personal data being divided into at least two categories having two different access conditions, each category being associated with a user's value,

5 - requesting access to the trusted centre by a third party to the personal data of a plurality of users, said request comprising search criteria and a third party value,
- executing by the trusted center the search criteria on the personal data of the users so as to determine a first set of users matching the search criteria for which the user's value is equal or lower than the third party value,
10 - returning the personal data of the first set of users,
- updating the counter of the first set of users with the content of the value of their respective personal data.

5. The method of claim 4, wherein the third party transmits a limit value with its request, and wherein a second set of users is selected among the first set of users
15 so that the sum of the user's value of each user of the second set does not exceed the limit value.

6. The method of any of the claims 1 to 5, wherein the request by the third party comprises filtering data, the step of transmitting the personal data comprises a step of filtering the personal data according to the filtering data prior to transmitting them
20 to the third party website.

7. The method of any of the claims 1 to 6, wherein it comprises the steps of :

- verifying at least some of the personal data,
- assigning a different user's value if the personal data have been successfully verified.

AMENDED CLAIMS

received by the International Bureau on 11 December 2012 (11.12.2012)

1. Method to control the access of personal data of a user by a trusted centre comprising at least one database comprising for a specific user, memory locations for personal data, access conditions associated to the personal data and management data comprising at least a counter,
 - loading by a user into the database of the trusted center, its personal data and assigning access conditions to said data, said personal data being divided into at least two categories having two different access conditions, each category being associated with a user's value,
 - requesting access to the trusted centre by a third party to the personal data of a plurality of users, said request comprising search criteria,
 - executing by the trusted center the search criteria on the personal data of the users so as to determine a first set of users matching the search criteria,
 - returning to the third party information showing the quantity of the first set of users matching the criteria, as well as the sum of the user's value of each user of the first set,
 - acknowledging all of part of the sum by the third party, thus defining a second set of users that can comprise all or part of the first set,
 - returning the personal data of the second set of user for which the sum covers the accumulated values of the extracted users,
 - updating the counter of the second set of users with the content of the value of their respective personal data.
2. The method of claim 1, wherein the information showing the quantity of the first set of users matching the criteria comprises the steps of :
 - grouping all users of the first of users that have the same user's value,
 - transmitting to the third party, the quantity of user per group.
3. Method to control the access of personal data of a user by a trusted centre comprising at least one database comprising for a specific user, memory locations for personal data, access conditions associated to the personal data and management data comprising at least a counter,
 - loading by a user into the database of the trusted center, its personal data and assigning access conditions to said data, said personal data being divided into at least two categories having two different access conditions, each category being associated with a user's value,

- requesting access to the trusted centre by a third party to the personal data of a plurality of users, said request comprising search criteria and a third party value,
- executing by the trusted center the search criteria on the personal data of the users so as to determine a first set of users matching the search criteria for which the user's value is equal or lower than the third party value,
- returning the personal data of the first set of users,
- updating the counter of the first set of users with the content of the value of their respective personal data.

4. The method of claim 3, wherein the third party transmits a limit value with its request, and wherein a second set of users is selected among the first set of users so that the sum of the user's value of each user of the second set does not exceed the limit value.

5. The method of any of the claims 1 to 4, wherein the request by the third party comprises filtering data, the step of transmitting the personal data comprises a step of filtering the personal data according to the filtering data prior to transmitting them to the third party website.

6. The method of any of the claims 1 to 5, wherein it comprises the steps of :

- verifying at least some of the personal data,
- assigning a different user's value if the personal data have been successfully verified.

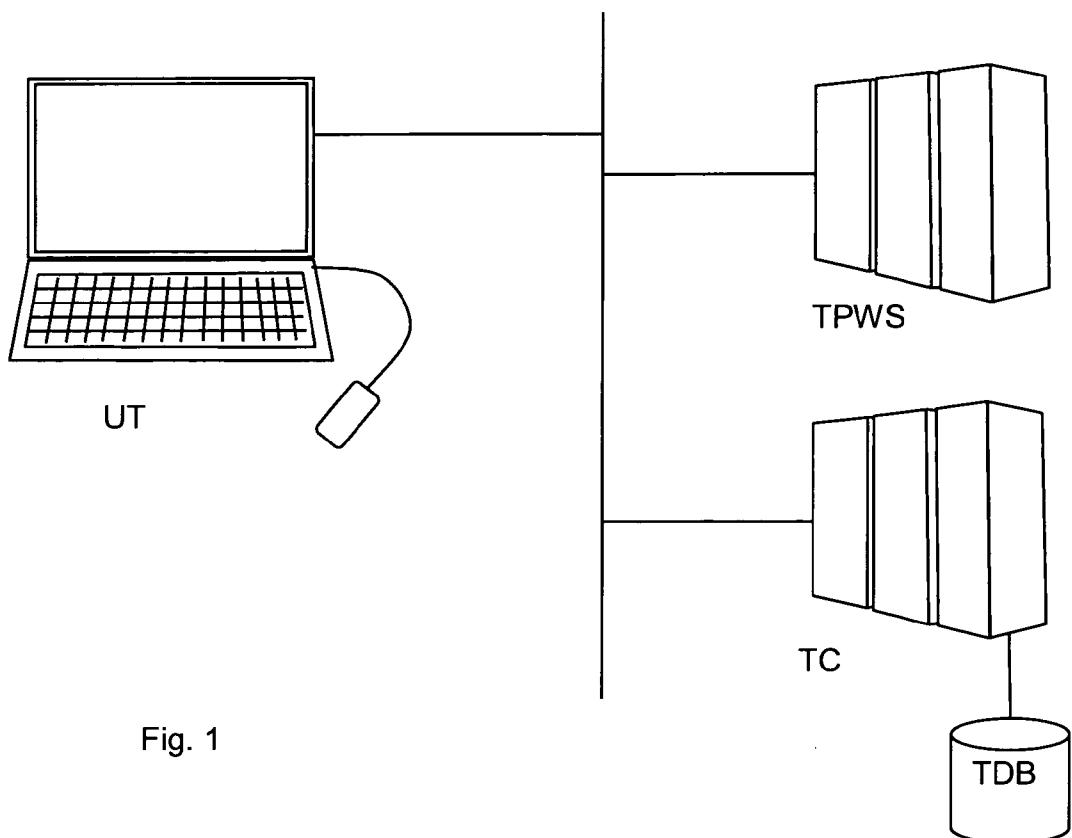


Fig. 1

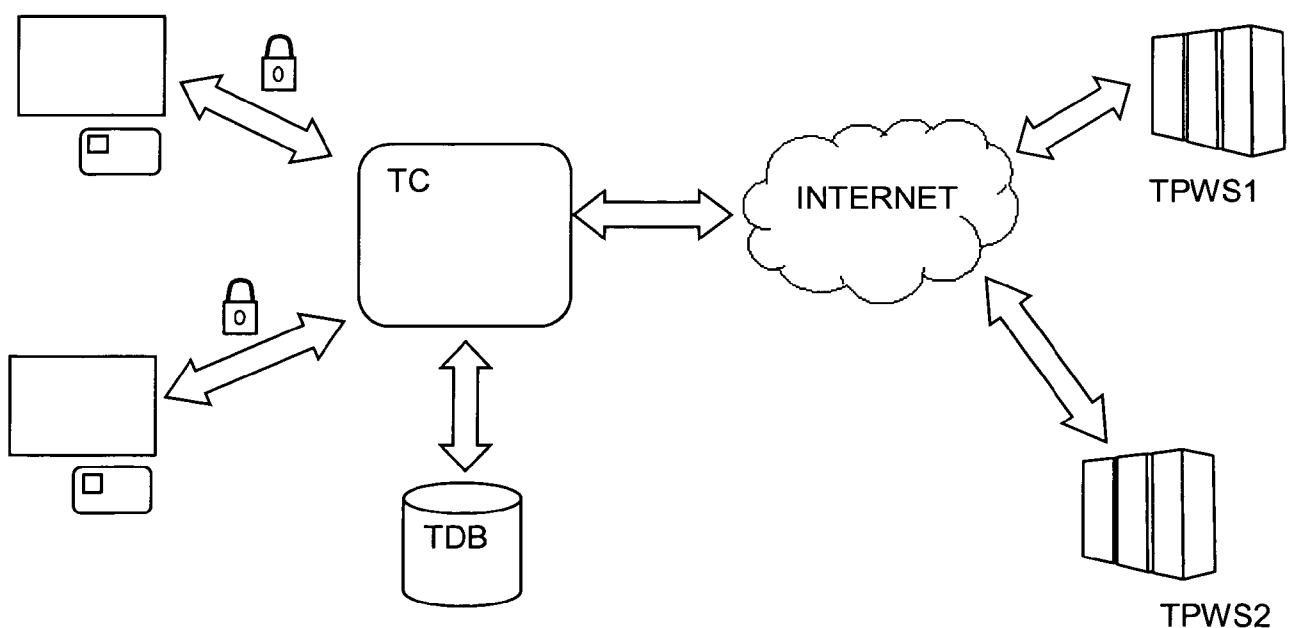


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/066837

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 G06F21/00
ADD.

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 G06F

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, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2010/088364 A1 (CARTER BERNADETTE A [US] ET AL) 8 April 2010 (2010-04-08) paragraph [0007] - paragraph [0008] paragraph [0015] - paragraph [0023]; figure 1 paragraph [0028] - paragraph [0033]; figures 2,3 ----- US 7 925 592 B1 (ISSA ALFREDO [US] ET AL) 12 April 2011 (2011-04-12) column 2, line 25 - column 3, line 15 column 7, line 9 - column 10, line 10; figures 2,3 -----	1-3,5-7
A		1-3,5-7



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

19 November 2012

26/11/2012

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

Raposo Pires, João

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2012/066837

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010088364	A1 08-04-2010	NONE	
US 7925592	B1 12-04-2011	NONE	