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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 January 2007 (04.01.2007)

PCT

(10) International Publication Number
WO 2007/002089 A2

(51) International Patent Classification:
G06F 17/00 (2006.01)

(21) International Application Number:
PCT/US2006/023982

(22) International Filing Date: 20 June 2006 (20.06.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/596,399 20 September 2005 (20.09.2005) US
60/595,283 20 June 2005 (20.06.2005) US

(71) Applicant *(for all designated States except US)*: **MYPUBLICINFO, INC.** [US/US]; 2020 North 14th Street, #700, Arlington, VA 22201 (US).

(71) Applicants and
(72) Inventors: **KRAFT, Harold** [US/US]; 3031 Millitary Road, Arlington, VA 22201 (US). **DANE, Pat** [US/US]; 801 North Caswell Street, Southport, NC 28461 (US).

(74) Agent: **CATAN, Mark, A.**; PROSKAUER ROAD, 1585 Broadway, New York, NY 10036 (US).

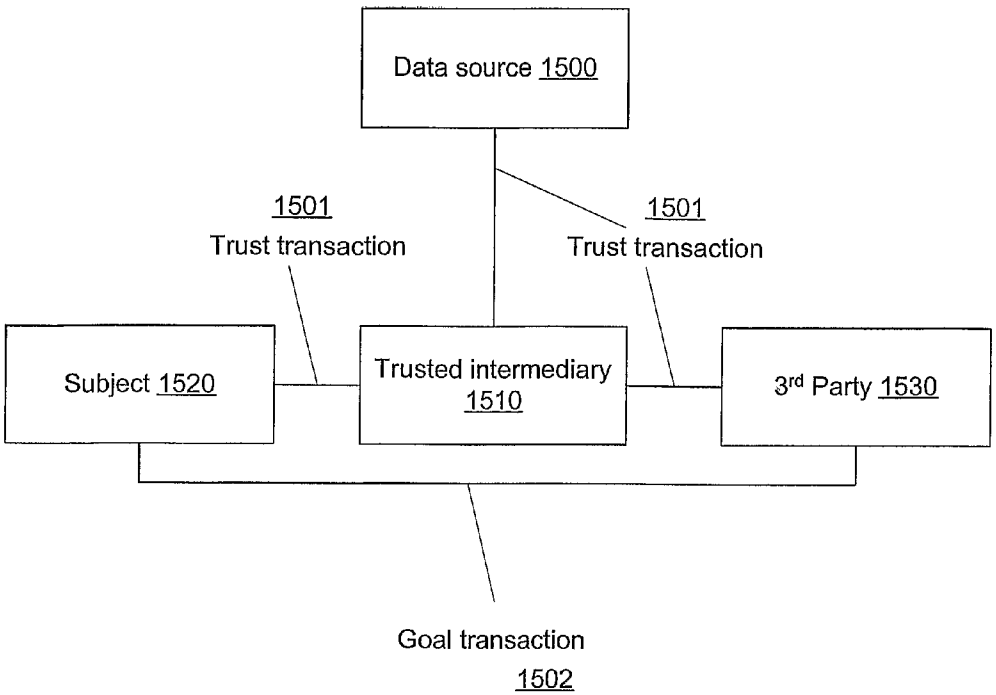
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, 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, HU, IE, IS, IT, LT, LU, LV, MC, NL, 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:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** IDENTITY INFORMATION SERVICES, METHODS, DEVICES, AND SYSTEMS



(57) **Abstract:** A system provides various features for facilitating the management of data used for facilitating trust in otherwise anonymous transactions.

WO 2007/002089 A2

Identity Information Services, Methods, Devices, and Systems

Background

It is a commonplace that individuals, corporations, and other legal and *de facto* entities make fraudulent claims about themselves. The industry in third-party background checks is, consequently, growing fast. In all types of personal, domestic, business, organizational, and legal relationships, there is a risk of people claiming to be someone other than who they are or of claiming characteristics or credentials they don't truly possess. Another risk that is related to identify fraud is the risk of having one's own identity stolen. An effective solution to one problem can help to ameliorate the other, assuming wide acceptance and use of the solution.

At the bottom of these issues is the concept of trust. The ability to trust the entities with whom one interacts facilitates the speed of transactions, reduces the costs of transactions – trust has real value in commerce and in personal situations.

Background checks are a staple tool used by prospective employers, private and public investigators and detective organizations, prospective spouses, and prospective creditors. Many services are available to generate reports providing information such as criminal background and financial credit-worthiness. More recently, the need for additional information such as verification of institutional credentials has been identified and mechanisms for providing such information proposed. The World Wide Web has spawned a variety of services allowing individuals and organizations to search for specific information about other parties, for example a family could perform a criminal background check on a prospective nanny or find out the owner of vehicle based on the license plate of vehicle identification number.

There is also a system called federated identity management, which allows users to use the same login credentials for different networks to perform transactions. FIM, different network owners trust each other to authenticate users, in a sense, telling other members that a user is or not.

Common devices used to create trust between parties in the electronic world are digital certificates, which are files that use cryptography to secure identification. There are client certificates, used by customers or employees to establish identity, and server

certificates, used by web sites to authenticate themselves to customers. Certificates also serve values in addition to authentication, including the creation of a vehicle to ensure that the data is not revealed or disclosed to unauthorized entities, protecting data from being corrupted or copy (integrity), proving that a party to a transaction actually conducted the transaction.

There is an emerging field of identity management that covers various related concepts that offer various tools for convenience, privacy, user-control, and security. Many in the identity management field foresee an important role for systems that make us of objective information sources that contain information about individuals and other entities and use that information to facilitate transactions. An example is where a user needs to prove some piece of information about himself or herself, such as age, state of residence, etc. and authorizes a trusted intermediary to transmit that information to the a third party that needs to confirm the information. As such systems become more important, the integrity of the data in the information source becomes more and more important in the lives of any entities who are the subjects of such information and who rely on these intermediary facilities to perform transactions with others. For examples of such systems, see US Patent Publication Nos. 20042802841665 for "Method and system for enroll-thru operations and reprioritization operations in a federated environment;" 20060130065 for "Centralized identity management system and method for delegating resource management in a technology outsourcing environment," 20060129817 for "Systems and methods for enabling trust in a federated collaboration," 20060123476 for "System and method for warranting electronic mail using a hybrid public key encryption scheme," 20060075461 for "Access authorization having a centralized policy," 20060074863 for "Method, system, and apparatus for maintaining user privacy in a knowledge interchange system," 20050246770 for "Establishing computing trust with a staging area," and 20050223217 for "Authentication broker service;" which are incorporated by reference as if fully set forth herein.

Summary

A system for showing information relating to a subject (i.e., a person, a legal entity, an institution, or any other legal person) to a user (who may be the subject or a

third party) may be based on primary and secondary sources of data. Examples of primary data sources include

Data sources that may be queried, either directly or through intermediate aggregators, include, for a few examples:

- Federal, State and County records
- Financial records like bankruptcies, liens and judgments
- Property ownership records
- Government agencies, government-issued and other licenses
- Law enforcement records on felony and misdemeanor convictions

UCC (Uniform Commercial Code) records that reveal the availability of assets for attachment or seizure, and the financial relationship between an individual and other entities. Examples of secondary data sources include data aggregation services which support background checks or which provide authentication functions or trust services in e-commerce transactions. An important example of a secondary source is a data store operated by a service provider who acts as a trusted intermediary to facilitate transactions, such as computer-based transactions.

A user may desire to review data from the primary and secondary sources determine if the data is accurate, for example, a user concerned about possible identity theft or the possibility of being confused with a terrorist or criminal. Another type of user might be interested in the information from such sources because s/he is contemplating a transaction with the person and wants to verify information about the subject, for example, a background check on a prospective employee or confirmation of the authenticity in a transaction.

Much of the present document is concerned with augmenting and verifying the accuracy of such data, to expose and/or correct discrepancies and or otherwise take steps to correct misinformation held in records relating to the subject. Such features may help to provide earlier notification of theft of the subject's identity or fraud involving the subject.

In the area of identity theft, subjects may need to manage and mitigate different kinds of risk, for example, the risk of corrupt, missing, or information erroneously attached to their identities which may be stored in the primary and secondary types of

sources. A subject's ability to check their information can provide not only the ability to avoid confusion by third parties, such as prospective employers, but also an indication of fraudulent use of personal information such as would attend an instance of identify theft. Armed with such information, subjects can takes steps to protect their identity from further exploitation, mitigate future risk, and repair damage done by identity theft. Also, the subject's ability to perform transactions which rely on these data can be protected.

As described below, a Public Information Profile (PIP) may be generated, which may serve as a comprehensive report or body of data summarizing the information stored in primary and secondary data sources and which may otherwise be available to others about the subject. It is envisioned that such a PIP would be generated by the subject for his or her own use. In embodiments, a system may sift through many, (e.g., 10 billion records) housed and administered by one or more data aggregators and culled by them from various public sources. In embodiments, a report is generated from these records using a networked architecture and delivered to a user (the subject of the search) via a terminal. In this example, the system would assembles this information into a single document (the PIP) which may be delivered online as an html or pdf type document or printed and mailed to a user, for example.

Various means of authentication may be provided to prevent someone other than the particular subject of the research from generating that subject's PIP. A preferred mechanism uses identification information about the user and queries one or more data sources for further information. Then the system generates a quiz based on this information to verify the contents of this further information. For example, the quiz may ask the user to indicate which of a list of addresses was a former residence of the user. The question can be generated as a multiple choice question with "none of the above" being a choice, to make it more difficult. Other kinds of questions can be based on the identity of a mortgage company, criminal records, or any of the information the system accesses.

In embodiments, the PIP is generated from a secondary source the collects information from primary sources and makes it available without having to go to the many primary sources. In the embodiments, the system may generate a PIP which

includes a form to accept data from a user indicating that certain data is questionable or indicates misinformation about the person or that some specific piece of data is missing. For example, a criminal conviction might appear on the PIP which could mistakenly be associated with the subject or a piece of real estate the subject formerly owned could be missing from the PIP.

In these embodiments, the user feedback indicating a question about the report contents may be used to generate a further query to primary sources. Many problems can occur in the uptake of data from primary sources to the secondary aggregators used to generate the reports. So a query of the primary sources may indicate the source of the erroneous or missing data as being due to an error in the secondary data source. Since the primary is more authoritative, the correct primary data may be delivered to the user in a second report which juxtaposes the primary and secondary data. The second report may include the subject's own comments in juxtaposition, for example, explanations for certain events with citations to supporting data may be entered and included in the report. These "annotations" may play a role in performing transactions where the system may provide the annotations as qualifiers to other information used in the transaction.

In alternative embodiments, rather than querying primary sources in response to a subject's indication of questionable data, the primary sources may be queried based on a schedule of sensitivity, degree of risk imposed by errors, or likelihood of errors. For example, if the first query of the secondary source turns up criminal records that are closely associated with the subject, for example based on an identical name, the primary sources in the associated jurisdiction may be queried to provide verification or highlight a discrepancy in the data or confirm or refute the relationship between the data and the authentic subject.

Another alternative may be to limit the scope of search of primary sources based on "bread crumbs" left by the subject throughout his life. For example, the primary sources for each state the subject has lived in (as indicated by the query result of the secondary source) may automatically be queried, rather than just relying on the secondary sources. Yet another alternative is to offer the user, who would also be the subject, a form to ensure that the data obtained and used to query the primary sources

is complete. For example, the user may be shown a list of states in which the subject appears to have lived based on the first query of the secondary source and asked if the list of states is complete. The user may then enter additional states as needed and the primary sources queried based on the complete list.

Yet another alternative may be to query both secondary and primary sources. This may have value for a user if the secondary source is one that is routinely used by third parties. Discrepancies between the primary and secondary sources can provide the user with information that may help him answer or anticipate problems arising from third party queries of the secondary source. For example, if the user applies for a job and the prospective employer obtains data from the secondary source, the user may be forearmed with an answer to any questions arising about his background. For example, the user may note on his application that there is corrupt data in the secondary source regarding his criminal history. Note that the alternatives identified above may be used alone or in combination.

The primary sources may be considered more authoritative since any data in the secondary sources may be the result of transcription errors, data corruption, or other process that distort data aggregated from the primary sources. A subject concerned about misinformation being obtained and acted upon by an interested third party (such as one involved in a transaction with the subject) may be offered by the user to the third party in some form. For example, a certified report showing the report fleshed out with data from both the primary and secondary sources according to the above may be generated by the system.

According to additional embodiments, the second report, with primary as well as secondary data and also with user-entered annotations and citations, may be generated by the user and printed. Reports or other kinds of transaction data may also be generated by third parties using an online process. For example, the system may store the complete second report after querying the primary sources and adding user annotations. The report can be generated by the user or by a third party with the user's permission and under the user's control, for example, by providing the third party with a temporary username and password provided on request to the user by the system and providable by the user to the third party. Alternatively, the data involved may be used in

the mediation of a transaction with the subject. The credibility of the report stems from the fact that it cannot be altered directly by the user, the owner of the system deriving much of its value from its integrity as well as the annotations and additional information provided by users.

Also, information for which there is a discrepancy between primary and secondary data may be submitted by the system operator to operators of the secondary source or sources. This information may be used to alter the secondary source data thereby to remove the discrepancy. Annotations and further citations submitted by the user through the system may also be transmitted by the operator of the system to the operator of the secondary source(s) for purposes of correction.

A user may subscribe to a service offered by the system, for example by paying a one-time fee or a periodic fee, which allows the user to obtain and recompile information. In addition, according to a similar subscription model, the user may receive periodic, or event-driven change reports which indicate changes in the content of the user's PIP. The change report may be delivered as full report with changes highlighted or as just a report indicating changes that have occurred. During the period of the subscription, the system may compile and keep a record of changes so that an historical record may be created and accessed and reviewed by the user. For example, the user may obtain change reports between any two dates.

Preferably PIP or associated information are provided to highlight data that are particularly sensitive or important and also to indicate the relevance of, or what to do about problems with, each item of the data in the PIP. The PIP may include, along with a detailed listing of findings, a narrative, automatically generated, which discusses the most salient features of the PIP. Such a narrative may be generated using template grammatical structures in a manner used by chatbots (chatterbots) for example, see US Patent, 6,611,206, hereby incorporated by reference as if fully set forth in its entirety, herein. Also, preferably, PIPs will indicate what search criterion was used to retrieve the record. In querying databases, there is no one unique identifier of a person who is the subject of the search. The person's name, social security number, or other information may be used alone or in combination with other data. Also, close matches to the name may be used. A user reviewing his report may be interested to know how

the record was associated with him and this may be indicated by the PIP overtly or conditionally, such as by a hyperlink button or mouse-over balloon text, for example.

Various objects, features, aspects and advantages of the present invention will become more apparent from the following detailed description of preferred embodiments of the invention, along with the accompanying drawing.

Brief Description of Drawings

Fig. 1 illustrates a network or Internet architecture for implementing various features of the present inventive embodiments.

Fig. 2A illustrates an embodiment in which a public information profile report may be generated from a secondary source, such as a data aggregator.

Fig. 2B illustrates an example of a public information profile report which may be generated according to inventive embodiments described in Fig. 2A and elsewhere in the specification.

Fig. 3 illustrates a quiz technique for authenticating a user.

Fig. 4 illustrates an embodiment in which a change report is generated from a user profile and a public information database.

Fig. 5 illustrates a system and method for generating an augmented public information profile report in which questionable information is fixed and/or annotated.

Fig. 6 shows a complete PIP illustrating an embodiment of a report form.

Fig. 7 shows a complete PIP illustrating an embodiment of a fix report.

Fig. 8 shows a portion of a PIP embodiment relating to real estate residences purchased.

Fig. 9 illustrates a portion of an embodiment of a list of data sources accessed.

Fig. 10 illustrates other information that may be included in a PIP.

Fig. 11 shows an example process for searching a database in which the search query is made broader by an iterative process that derives alternative search criteria.

Fig. 12 shows an embodiment of a portion of a public information profile (PIP) which summarizes the contents obtained.

Fig. 13 shows an embodiment of a portion of a public information profile (PIP) which provides links to different portions of the PIP.

Fig. 14 shows an embodiment of a portion of a public information profile (PIP) which provides information and link controls for assistance regarding certain elements of the PIP.

Fig. 15 shows an embodiment of another portion of the public information profile (PIP) which provides information and link controls for assistance regarding certain elements of the PIP.

Figs. 16A and 16B show collapsed and expanded views of criteria used to show records obtained (a similar embodiment may be included as well to show information about the sources of the information).

Figs. 17 and 18 illustrate a PIP format feature that helps users understand when discrepancies may arise between one or more data sources and how to cure them.

Detailed Description of Drawings

Fig. 1 illustrates a network or Internetwork architecture for implementing various features of the present inventive embodiments. The inventive embodiments concern reports of information from content databases, for example public records of interest to the subjects of the reports, for example, individual consumers. Examples of public records include credit profile data, criminal convictions, financial records such as bankruptcy, and property ownership records. A user 215 may request information from one or more service providers 216 through a wireless 200, or fixed 220, 222 terminal. The request may be entered in a form, for example an html form generated by a server 221 and transmitted to the terminal 200, 220, 222 via a network, internetwork, and/or the Internet 210. Data submitted by the user (or interested third party, assuming the subject of the data is said user) 215 may be transmitted from the terminal 200, 220, 222 via a network, internetwork, and/or the Internet 210 to the server 221 (which may be the same or a different server or servers) and used to generate a query. The query may be generated on one server 221 and transmitted, via network, internetwork, and/or the Internet 210, to another server 221 and in response data obtained as a result of the query and also transmitted, via a network, internetwork, and/or the Internet 210, to the user or third party 215 at a corresponding terminal 200, 220, 222 or some other location, for example a permanent or semi-permanent data store for future access (not

shown separately but structurally the same as servers 221). The network, internetwork, and/or the Internet 210 may include further servers, routers, switches and other hardware according to known principles, engineering requirements, and designer choices.

Fig. 2A an embodiment in which a public information profile report may be generated from a secondary source, such as a data aggregator. The arrows illustrate data exchange processes which are described in the text. The entities represent computers, servers, and data transfers may occur through networks or internetworks, such as the Internet using any appropriate known protocols. Multiple primary sources 125 of information are queried by the owner of one or more secondary sources 115 to aggregate the contents of the primary sources and make the data available to customers of the owners of the secondary sources (not shown). For example, the secondary sources 115 may include identification and credential verification service or credit bureaus. Secondary sources 115 may provide rapid and complex searches by subscribers. For example, entities such as government offices, the FBI, prospective employers, etc. may subscribe to services of the secondary source 115 providers to do background checks on individuals of concern to the entities. Such individuals may include job applicants, proposed business contacts, constituents, criminal suspects, opposing political candidates, individuals who are parties to a transaction with the subject, etc.

When a secondary source 115 obtains data from primary sources 125, the data may suffer any of a variety of changes, such as data corruption, transcription errors, deliberate data manipulation, etc. These may occur in a process of data transfer from the primary source 125 or within the secondary source 115. These changes are represented figuratively by the operator 120. A Public Information Profile (PIP) service which has subscribers who are individuals concerned about their own personal information and misinformation which may be available through the secondary 115 or primary 125 sources may obtain data directly from the primary 125 and/or secondary 115 sources and compile a report 110, or who want to convey authenticated information to a third party in furtherance of a transaction. The report contains all information generated from the primary 125 and/or secondary 115 sources resulting from a query

generated by a query process 130 which uses information from a profile form 105 providing data about a user. Output could also be in the form of a request for confirmation of a particular piece of information – a part of the profile – rather that the report content itself. For example, the output could just be effective to confirm a claim about the subject.

Examples of primary and secondary sources 115 and 125 include:

- Property ownership records, real estate records,
- Government-issued and other organization and professional licenses and registrations and professional and educational certifications, degrees, etc. These might be found government, employer's or other entity's background information store.
- Law enforcement records on felony and misdemeanor convictions. Criminal records and special offender (e.g. sex-offender) registered lists. These include criminal convictions – including misdemeanors and felonies. These records might be found in a government, employer's or other entity's background check.
- Financial records like bankruptcy, liens, judgments: These include bankruptcies, liens, and judgments awarded against an individual or individuals. These records might be found in a government, employer's or other entity's background check.
- PACER: Public Access to Court Electronic Records (PACER) is an electronic service that gives case information from Federal Appellate, Federal District and Federal Bankruptcy courts.
- UCC (Uniform Commercial Code) records that reveal the availability of assets for attachment or seizure, and the financial relationship between an individual and other entities. These include public notices filed by a person's creditors to determine the assets available for liens or seizure.
- Secretary of State: including corporate filings identified by the names of agents/officers. An example of a web site offering such information is NY's department of state web site located at: http://www.dos.state.ny.us/
- Internet search: matches from databases that may match or cite your name or names similar to yours, from Web search engines, usenet newsgroups, or any other Internet-accessible resource.

- Personal Details: matches from databases that are associated with your name or names similar to yours, your past or present address and telephone, your SSN, your relatives, or even people that you have been associated with.
- Insurance claims databases, such as CLUE, which store information about insurance claims made by individuals and organizations.
- Credit Header Data: the addresses associated with your Social Security Number and name in credit reports. The address history in your PIP can be 10-20 years old. These records might be found in a government, employer's or other entity's background check.
- HUD: Department of Housing and Urban Development (HUD) or Federal Housing Administration (FHA) insured mortgage, subject may be eligible for a refund of part of your insurance premium or a share of any excess earnings from the FHA's Mutual Mortgage Insurance Fund. HUD searches for unpaid refunds by name.
- PBGC: Pension Benefit Guaranty Corporation, collects insurance premiums from employers that sponsor insured pension plans, earns money from investments and receives funds from pension plans it takes over.
- Financial and credit data as provided by the three major credit bureaus.
- Census data
- Voting records
- Telephone disconnects and other telephone company data
- United States Postal Service Coding Accuracy Support System (CASS) is an address correction system which compares an address to the last address on file at the USPS for the recipient.
- Email databases.
- Other Fraud Databases, such as maintained by data aggregators, that associate identifiers, such as a particular physical address, with known risk of fraud.
- Telemarketing and Direct Mail Marketing databases.
- Retailer databases including customer loyalty databases, demographic databases, personal and group purchasing information, etc.
- Warranty registration databases.

In the embodiment of Fig. 2A, data is preferably derived from the secondary source or sources 115 to allow the report 110 (e.g., a PIP, validated data, or validation data) to be generated quickly and consistently. This is because the primary sources 125 can be numerous and diffuse; that is, they may be scattered at many different locations and in various states of accessibility. If one were to rely on the primary sources 125, the report 105 would take longer and it would be inconsistent in terms of scope because the unavailability of certain databases. However preferable, the inventive embodiments are not limited to querying only a secondary (aggregator) source. In addition, the secondary source or sources 115 may or may not include content aggregators. They may include content enhancers, i.e., ones which take data from a single source, but which enhance it in some way, for example by holding data for longer periods of time, making data from primary sources 125, which is ephemeral, more permanent. The service provider that supports the query process may also store data and so may be regarded as a secondary source 115. For example, the annotation data might be stored by the service provider.

Where various sources contain identical primary information, the elements of this information may be juxtaposed in the PIP for comparison. For example, the PIP may highlight those information elements that contain identical information but with discrepancies. The sameness of the data may be determined based on the information itself or from descriptive information from the data source. For example, an address record may contains the same address with different valuations of the price paid for the property on a particular date. The discrepancy may be highlighted in the report by lining up the identical records, such as in adjacent rows of a table with the corresponding elements aligned in columns. Only the differences in the primary and secondary data may be shown with only one instance of the common information. Preferably, the sources of the information would be indicated as well. In this way discrepancies in the data may be discerned easily by the user.

In terms of a method, a user authenticates himself by logging into the query process 130 which has generated a form 105. The form accepts data from the user identifying him and the subject's data is used by the query process 130 to generate a query of the secondary source 115. The identifying data accepted by the form may

include authentication information that includes private information that the user would normally keep secret, such as his social security number. The query process 130 may use discrepancies in the data as a basis for rejecting the request for a PIP or other data by generating an appropriate user interface element such as a dialog box. The secondary source 115 generates a set of data from the query by filtering and sorting its internal database and transmits them to the query process 130 which then formats and adds additional data (described below) to generate the report 110. An element of the method is content aggregation performed by the secondary source 115 in which data is regularly obtained by an internal query process (not shown) is applied to the primary sources 125 to obtain comprehensive compilations of data which are stored by the secondary source 115.

Fig. 2B illustrates an example of a public information profile (PIP) report which may be generated according to inventive embodiments described in Fig. 2A and elsewhere in the specification. A navigation header 248 includes categorical areas 250, 255, and 262 which may be hyperlinked, with subcategory links 252, 257, and 262. Categorical areas 250, 255, and 262 represent assets, legal and license records, and bread crumbs, respectively. The meanings of the categories should be apparent from the text subcategory links 252, 257, and 262 shown in the drawing and from the details illustrated further on. The bread crumbs area is for information that can be compiled from various sources that represent random information relating to the user, for example, it may be such as an Internet search on the user's name or other identifier would provide.

Area 262 is a summary header providing identifier information about the user who is the subject of the report, a summary of the results, and date and time information or other information that qualifies the report. The summary of the results may include subject matter categories 294 ... 296 with corresponding results 295 ... 299 and corresponding explanations 297 ... 298. The categories 294 ... 296 may follow the categories 250, 255, 260 and/or subcategories 252, 257, 262 described below. The results 295 ... 299 may simply indicate the number of positive hits (records associated with the user) found within each category. Respective explanations 297 ... 298 may

indicate what search criteria produced any positive hits or may summarize all of the criteria which were tried. For example, it may recite as follows:

- 5 properties found based on SSN, in MD, NY, & VA. 1 additional found based on "John Public" in VT. Tried SSN, "John Quincy Public;" "John Q Public;" and "John Public" in all sources listed in summary section.
- 0 properties found based on SSN, "John Quincy Public;" "John Q Public;" and "John Public" in all sources listed in summary section.

where "SSN" stands for social security number.

The summary header 262 may also include information about limits placed on the content of the report, who is authorized to read it, etc. Area 264 indicates a blurb or a link to the same to describe in summary fashion how to use the report, what its limits are, and what to do about misinformation appearing in the report, or failing to appear in the report.

Area 268 is the asset category section and it includes the section 270, which is the first section delivering results from a search. This section 270 is a real property report and includes subsection 272 which describes information about the first property, such as transaction data, property description, mortgage companies, parties involved in the transaction, etc. The section 272 may accompanied by graphics such as a satellite photo 271 and street map 273 of the property and surrounding area. Also illustrated is a citation/criteria block 277 indicating the particular source of each item of information and what criteria produced the positive result. The citation/criteria block 277 may be provided on a record by record or field by field basis. It may indicate a category of the secondary source 115 or a particular primary source 125 or category (part of the source database) from which the associated data item originated. Other items such as assessed value, values for comparables in the neighborhood, etc. may also be provided. The ellipses at 274 indicate that many records may follow as appropriate. After the record data, at 276, the list of sources searched may be indicated. The list of sources 276 may identify primary sources 125 or secondary sources 115 or portions thereof, whether the data was derived through the primary or secondary source. For example, the secondary source 115 may identify the primary source from which a datum was originally obtained by the secondary source 115. This original source

information may be passed through the secondary source 115 and the data attributed to the primary source even though, for purposes of generating the report, it was derived from the secondary source 115.

One of the important pieces of information included in a PIP is what it does not show, that is, the lack any hits after a particular database is searched. A consumer may be just as interested in a failure of the PIP to show a record as in a record showing up which is either wrong or should not be identified with the user. Thus, the list of data sources accessed is a useful component of the report and may therefore be included in the body of the PIP.

Further sections and records such as the UCC report area 278, Craft report area 282 to show records such as for planes and boats registered to the user, legal and license area 286 with criminal records 288 may include corresponding lists of data sources 280, 284, and 290. Further records grouped by category and listed as indicated in the navigation header 248 may be shown as suggested by the ellipses 282.

The entire report of Fig. 2B may be delivered as a digital document, a printed document, or an html page or any other means. It may be encoded on a smart card or other portable data store. Authentication information may be included in the report, for example, a hologram seal on a printed report, to provide some verification capability that the report is true to the information and reporting done by the service associated with system Fig. 2A.

Fig. 3 shows an embodiment in which feedback is obtained to further confirm the identity of a user. Here, as in further embodiments, like numerals indicate similar or identical components and are not redundantly described for that reason. In this embodiment, after identification/authentication information is obtained through the form 106, the query process 131 calls up information from the secondary source 115 and creates a quiz. The quiz tests the identity of the user by asking questions about information the user would likely know but someone other than the person would not. This guards against someone benefiting from finding or stealing the user's wallet or other personal effects containing personal information. For example, the quiz may ask the user to indicate which of a list of addresses was a former residence of the user. The question can be generated as a multiple choice question with "none of the above" being

a choice, to make it more difficult. Other kinds of questions can be based on the identity of a mortgage company, criminal records, or any of the information the system accesses. The query process 131 may employ predefined rules for the purpose of generating the quiz. For example, the process 131 may rely on a randomized selection of data such as mortgage company, old addresses, previous employers, locations where craft were registered and what kind, size of houses previously owned, etc. The query process 131 may further rely on the effectiveness of candidate discriminators to distinguish among possible users, for example, by doing a search on individuals similar to the person identified by the identification/authentication information and then basing questions on what makes each unique compared to the others. This is a more flexible approach and can be implemented using a simple frequency filter that identifies the questions whose answers are least likely to be shared by two or more in the search result of similar individuals.

Fig. 4 illustrates an embodiment in which a change report is generated from a user profile and a public information database. The process and system represented by Fig. 4 is similar to that of Fig. 2A, except that after the query process 170 authenticates the user and generates and transmits a PIP, at least some parts of the PIP are stored in a profile 157 associated with the particular user. Then, periodically, the query process 170 queries the secondary source 115 and compares the resulting filtered set of data to the data stored in the profile 157. In an embodiment, any changes in the secondary or primary sources indicated by a comparison between baseline data stored in the profile 157 and the most recent query of the secondary and/or primary sources 115, 125 are identified and shown in a change report.

In another emobodiment, a query process 170 may follow a pattern recognition process 165 to identify certain kinds of changes. For example, the pattern recognition process 165 may be trained to identify traces of fraudulent actions. These patterns may be diffuse, such as certain kinds of monetary withdrawals that look like someone trying to hide under the radar or focused such as the registration of a vehicle in a state in which the user has no previous ties. When the pattern recognition process 165 identifies one or more events of interest, it may generate a notification to the user, such as by SMS messaging or email and provide access to a report providing details of the

event(s) that triggered the notice, as represented by change report 160. Note that similar pattern recognition processes may be used to identify noteworthy patterns or trends in the PIP as well as to generate change reports, as described further with reference to Fig. 5.

Change reports and triggers for change reports may include the following.

Change reports providing background checks on

- employees and delivered to an employer;
- spouses and delivered to a spouse;
- business partners and delivered to partners;
- principals of competitor organizations and delivered to competitor;
- students and delivered to headmasters;
- parolees and delivered to parole officers or court clerk;
- neighbors and delivered to neighbors; etc.
- Change reports may be generated and transmitted to subscribers
- On a periodic basis;
- In response to changes detected in consecutive PIPs;
- In response to specific criteria such as the appearance of a criminal record or civil judgment;
- In response to specific events; etc.

Change reports may include

- Only changes from one report to the next;
- All information normally in a PIP, but highlighting changes from one report to the next;
- All information normally in a PIP, but highlighting changes and/or content considered relevant according to subscriber's personalized policies such as an interest in only legal issues or financial issues related to the target;
- Only certain classes of information, such as legal and financial, but all information in occasional reports.

Change reports may be delivered

- On mobile devices;
- In email by way of a link or included in content;
- By mail, telephone, or other medium.

Fig. 5 illustrates a system and method for adding information to the secondary sources in which questionable information is fixed and/or annotated. A profile form 105 is filled out by the user as in the embodiment of Fig. 1A and a query process 325 generates a report form 315 which contains a PIP with a form for feedback. The form may be integrated into the PIP, for example form controls in an html-delivered PIP format. The report form 315 is designed to allow the user to indicate questionable items in the PIP. For example, each data item may be provided with a check box or set of radio buttons to indicate that the data item is believed to be wrong for some reason. The report form 315 may include multiple iterations (a second html page, for example, in response to the user submitting the first form) to request further information about the supposed errors. For example, the second form 315 may ask whether an address that was flagged by the user in the first form 315 was the wrong address or contains a typo. The first form may include controls to allow the user to indicate that a data item is missing, for example, an old paid up mortgage is not listed.

When the query process 325 receives the form 315 and any further iterations of it, it generates one or more queries of the primary sources 125 associated with the data that were indicated as erroneous or incomplete. The box labeled primary sources 125 may be viewed as encapsulating any access devices such as a web-interface to allow queries to be satisfied. Many governmental organizations provide such services for free. But a manual search may also need to be done. With the additional data from the primary source, the query process 325 generates a new fix report 305 that contains both the secondary source data and the primary source data, preferably in juxtaposition for comparison. The fix report may contain only the flagged data items or it may be a complete PIP with the additional information shown. Preferably, in a complete PIP, the verified data items are highlighted, such as by using a colored background.

Information indicating noteworthy or otherwise significant information can be derived by making comparisons and/or detecting patterns in data from multiple sources such as:

- Comparing data from a database with lesser authority with one with a greater authority such as comparing a secondary source with a primary source, to determine if a source may be wrong.
- Looking for inconsistencies among data, including direct inconsistencies (such as above) and indirect inconsistencies. An example of this is where the demographics of subject are inconsistent with recent purchasing patterns. E.g., a young accountant with a family purchases aftermarket auto parts at a bricks and mortar retailer far from the subject's home address. For another example, if certain data tend to change at the same times: the telephone database should indicate that a subject's phone number has changed when the address changes, for example, and when it hasn't it's something that should be flagged in the PIP, change report, and/or alert. Yet another example is where different primary and secondary credit or merchant databases show instances when a "most recent" address for a name (with or without an Social Security Number and other identifiers) does not match from one data source to the next.
- Structural defects in data such as failure of uniqueness, such as more than one name associated with a Social Security Number or similar clusters of information that would indicate multiple instances of a an individual, for example identical name and age living at a single address at one time, but residing at more than one address at another time.
- Identifying data held by entities with known past instances of fraud such as massive theft of loss of information. Additionally, data storage entities that are popular targets of data theft or known to be vulnerable to data theft. For example, a large multinational bank may be a more common target for hackers than one with a purely local presence and difficult to access extraterritorially.
- Classifying data associated with a subject according to known patterns of fraud liability. For example, demographic data of a subject may, statistically, be associated with a higher incidence of fraud, for example addresses. This could happen where the trash of wealthy residents is a

known target of dumpster divers looking for sensitive documents that have put in the trash. Classification can be constructed using known collaborative filtering techniques, based on diverse sources of information even as divergent as voting records and census data. Although such records may not be updated frequently they can be used to generate classifications for subjects that are persistent. Data classification may be fuzzy in nature, and not a black and white indicator. For example, an examination of cell phone databases might indicate that a unique individual has more than one cell phone. While not a indicator of fraud by itself, it is noteworthy and, if combined with other information, it may provide a strong indicator of fraud or identity confusion problems.

Fig. 6 shows a complete PIP 370 illustrating an embodiment of the report form 315. A check box control 345 is shown as an example in the Asset section's real property section 365 adjacent an address 355. Also shown is a text box control 346 for the user to enter a comment about the particular piece of data, here, the address in this example. A user may check the check box 345 to indicate that information is desired to be submitted and enter text in the text box control 346 and submit the form 315 which is then processed by the query process 325. Other records and other information are indicated elliptically at 386, 390, and 395 including data sources accessed 375. The embodiment of the PIP 370 may be implemented as an html form so that it serves as both a report and form.

Fig. 7 shows a complete PIP 371 illustrating an embodiment of the fix report 305. As in the previous embodiment, it contains an asset section 376 with a real property section 366 with address information 355 of the report form 315 embodiment. Juxtaposed with address information 355 is address information 360, which originates from the search of the primary sources 125. The user's comment 397 also appears in a manner that associates it with the information that was questioned. In addition to a Highlighting 380 may indicate that information in the PIP 371 includes information that is revised, for example as shown here, the address information 355 and 360 are highlighted 380 to indicate that the additional address information 360 has been

provided. Also, the additional source of information 385; i.e., a direct query of the original source, may be shown in the sources listing 376.

Fig. 8 shows a portion of a PIP embodiment relating to real estate residences purchased. This is a snapshot of what might appear in section 270 in the PIP 248 illustrated and discussed with respect to Fig. 2B. Fig. 9 illustrates a portion of an embodiment of a list of data sources accessed. This is also a snapshot of what might appear in section, for example 276 or 284, in the PIP 248 illustrated and discussed with respect to Fig. 2B. Fig. 10 illustrates helpful information (e.g., as indicated at 292 in Fig. 2B) that may be included in a PIP.

Fig. 9 illustrates a portion of an embodiment of a list of data sources accessed. This may be provided as part of the PIP or in a separate document. It shows all data sources grouped and ordered by region for each category of data. For example, the illustrated one is a portion representing data sources for real estate information.

Fig. 10 illustrates other information that may be included in a PIP including instructions for what to do if certain kinds of false or misleading data are identified automatically or by the user. For example, as shown, contact information to allow the user to file a credit freeze with the three major credit bureaus may be provided. Other information and web controls may also be provided as described elsewhere in the present specification. Preferably such information is shown in the PIP itself with web navigation controls to make a long report convenient to review.

Fig. 11 shows an example process for searching a database in which the search query is made broader by an iterative process that derives alternative search criteria. A query process 405 generates a query as indicated at 420, for example, one including only a social security number to search a first database 415, in the present example one provided by an aggregator 415 of diverse primary data sources. The result of the first query is further information connected to the social security number. In the example shown, the further information includes names and addresses as indicated at 425. These may include a variety of names and addresses if the name has been misspelled, was changed, or a number of formats are used. The addresses and names may be run through a standardization process of filter 430 to conform the names and addresses to a standardized format to make essentially identical addresses appear the same. For

example, the post office provides such a filter for addresses. The duplicates are then eliminated in the list of names and addresses as indicated at 435 and the resulting list used as alternative query vectors for searching all the searched databases, including primary and secondary sources 410. The search results are then obtained as indicated at 445.

Note that the embodiment of Fig. 11 is not limited to names and addresses. Other kinds of search vectors may be used, such as driver's license number, biometric data, etc. Also, the filtering and duplication-elimination processes may be eliminated or altered to allow for misspellings in the records of the databases. The aim of the process of Fig. 11 is to obtain all the possible records associated with the user. Also, although the process is illustrated as querying an aggregator database with a first query and then querying other sources 410, it is possible to query primary sources and then aggregator sources of information or primary first and then, based on the result, aggregator databases.

Fig. 12 shows an embodiment of a portion of a public information profile (PIP) which summarizes the contents obtained. The portion, a header and navigation area 500 of a web page, for example, generated dynamically from the search result, includes a print control 515. Each of multiple sections, for example one indicated by a category label 530, correspond to a category of information returned by the search. Indicated alongside the category label 530 is a phrase (e.g., such as at 510) indicating the number of records found and information about the search, for example, the criteria used in the query. In the first example indicated at 510 16 addresses were found in the address history search by matching against social security number. A control to view the results is indicated alongside the portion 530 at 520. Other examples of criteria are indicated at 535 and 540. A header part 505 identifies the subject of the PIP. The header 500 may appear at the top of a long report which may appear as a single web page that is dynamically generated.

Fig. 13 shows an embodiment of a portion of a public information profile (PIP) which provides links to different portions of the PIP. This is an example of a navigation control in which all the different sections are grouped by a broader category such as indicated by the label 555. For each broader category, a link (such as indicated at 550)

for the portions of the report corresponding to each of a number of narrower categories are also provided. Preferably this navigation tool is shown at the top and links provided to it (or it is duplicated) at various parts of the report, which in practice, could be very long.

Fig. 14 shows an embodiment of a portion of a public information profile (PIP) which provides information and link controls for assistance regarding certain elements of the PIP. For each section of the report, various pieces of relevant information may be provided such as indicated (and self-explained) at 605, 615, and 610. In a preferred embodiment, a more detailed explanation of the nature of the records is shown in the corresponding section close to the corresponding group of records. This is a navigation expedient; namely, distributing the key relevant descriptions among the records in the report. Description and other information which are deemed key in the preferred embodiment are a detailed explanation of what the records are, where they come from, and why the records may include unexpected results. A short FAQ may appear in this same location. Similarly adjacent each record group, as in Fig. 16, information and link controls for assistance, such as indicated (and self-explained) at 620, 625, 630, and 635, regarding certain elements of the PIP may include an expandable list of data sources, or as indicated in Figs. 16 A and 16B an expandable list of criteria used to generate the search results may also be provided. Although it is preferred that this information and these controls be distributed in the report as shown, in alternative embodiments they may be provided in a single location in the report or on a separate page, which may be programmed to open in a separate browser window or browser tab.

Figs. 16A and 16B show collapsed and expanded views of criteria used to show records obtained (a similar embodiment may be included as well to show information about the sources of the information). Fig. 16A shows the list of criteria in an unexpanded state and Fig. 16B in an expanded state. The features are indicated (and self-explained) at 710, 720, 725, 715. The criteria 715, as discussed above, may include various alternatives of similar (overlapping) information such different references to the same address and the count of results. Queries that produce negative results are also shown by the column of records returned counts indicated at 725.

Figs. 17 and 18 illustrate a PIP format feature that helps users understand when discrepancies may arise between one or more data sources and how to cure them. In Fig. 18, a report (PIP) 7000 contains two records, each determined to pertain to the same person, event, or thing. For example, both can represent the same house. However, the records are not identical in content and contain contradictory information, such as who the owner was or whether a lien exists on the property. The contradictory information, indicated as Field 1 705 and Field 1 710 are formatted so that they are juxtaposed for easy comparison. To further highlight the contradiction, a highlight 750 is added such as a colored box, a border, or some other means. Also included is an instruction for responding to the discrepancy indicated at step 740 and a link to a site with further information for responding or further information about the problem, indicated at 745. Note that discrepancies can be shown without special formatting just by including otherwise identical records in the PIP.

Discrepancies can arise for example where a data aggregator makes a transcription error when copying information from a primary source. Also, when a record is not updated after a change of status, for example the title is not changed after the sale of a fractional interest in a house to a remaining spouse following a divorce. In Fig. 19, a process for identifying similar information and formatting the results for easy comparison is shown. In step S205 two databases containing information pertaining to a same person, event, or thing are queried and the results compared at step S215. At step S220, it is determined if information in the records pertains to the same person, event, or thing. For example, if the information relates to an address, the addresses are compared to see if they are the same or similar. Then, at step S230, if the comparison indicates the results pertain to the same person, event, or thing, normal formatting is applied at step S230 and in the alternative case, special formatting is applied at step S 235. The latter may include the addition of instructions and/or links as discussed with reference to Fig. 17.

The kinds of uses of a PIP or change report and the other services discussed above are many and varied even though we have emphasized personal identity protection. As noted above, all the features discussed with respect to a "user" may be provided to a third party where the user is the target of the information search but the

recipient is a third party. Examples of third parties who might use such a system, such as the change-report system of Fig. 4, for example, would be employers who wish to know of any information that might case an unfavorable light on an employee. Other examples include spouses interested in monitoring their spouse, patients monitoring doctors, business owners with regard to their business relationships, customers, etc. The examples are too numerous to list.

While there are known methods for evaluating the likelihood that fraud has occurred or is about to occur in various situations, most of them are processes that support and protect businesses, not individuals and fall within the class of processes known as data-mining. This area is known as fraud detection and they are of interest to banks and insurance companies, to name examples. Devices include predictive models of when fraud has occurred, or is about to occur, to allow businesses to respond, such as by locking a credit card or bank account until the owner confirms a transaction.

With regard to individuals, it is possible to subscribe to a service that alerts consumers to possible fraudulent activity related to their charge accounts. To help consumers anticipate how their behavior may affect their susceptibility to fraud, there is only good advice. As part of a service for overall identity protection, a method of predicting susceptibility of an individual to fraud and giving the individual an opportunity to proactively change his personal circumstances and behavior and external circumstances to reduce it.

Fig. 19 illustrates, at a high level, a kind of transaction contemplated in the foregoing discussion in which a subject 1520 is party to a goal transaction 1502 with a third party 1530, such as a job application, a purchase, an information request, or any kind of transaction where the subject 1520 must authenticate or prove a characteristic of the subject 1520 or the subject's identity. The goal transaction could be a non-electronic transaction such as a paper-based job application or an electronic transaction in which the goal transaction is completed electronically, such as registering for a class online or making an application for some kind of credential, or even making an e-commerce-type purchase. Here a trusted intermediary 1510 provides a service, such as one discussed in one or more of the patent documents incorporated by reference above. The trusted intermediary 1510 is a process hosted and maintained by a

disinterested entity and which has access to data sources and conveys information to facilitate the goal transaction 1502.

The trusted intermediary 1510 process may be provided by the same entity as provides the query process 325 in the example of Fig. 5 and others. The data source 1500 is the data store (such as primary and secondary sources discussed above). The subject's ability to conduct the goal transaction is affected by the quality of the data in the data source 1500. The foregoing embodiments provide the ability to maintain the data and also augment them as discussed. For example, the trusted intermediary may supply qualifying data such as the annotations submitted by the subject 1520, discussed earlier, independently of the process of Fig. 19. The trust transaction 1501 may include the actual annotation or an indication that the annotation exists, for example.

Although the present invention has been described herein with reference to a specific preferred embodiment, many modifications and variations therein will be readily occur to those skilled in the art. Accordingly, all such variations and modifications are included within the intended scope of the present invention as defined by the following claims.

Claims

1. A method of providing a validation for a claim relating to a person, comprising the steps of:

at one or more server stations of a computer network having access to personal information relating to the person, sending to a terminal of the person, for display thereat, a selected item of the personal information; and

at the one or more server stations, accepting, from the terminal, an indicator of annotation information correlating the further information with the selected item of information and storing at the one or more servers both the annotation information and selected item of the personal information for use by a third party in a transaction between the person, or agent of the person, and a third party.

2. A method as in claim 1, wherein the personal information about the person includes information uniquely identifying the person.

3. A method as in claim 1, further comprising the person or an agent of the person performing a transaction between the person or agent and the third party, the transaction requiring the determination of the accuracy of a claim relating to the person being made by the person and transmitting at least the annotation information to a terminal of the third party.

4. A method as in claim 1, further comprising generating a tamper-resistant indicator of the claim relating to the person.

5. A method as in claim 1, wherein the personal information relating to the person is stored at multiple databases including databases under control of government authorities.

6. A method as in claim 1, further comprising accepting profile definition commands to define a profile layer which indicates profile data, which is dependent on the personal information, that may be used in a class of transaction, the profile definition commands including an indicator of a definition of the class of transaction.

7. A method as in claim 1, further comprising:

registering for an identity management service that provides authentication and validation of the claims to third parties with whom the person transacts, the one or more servers being under the control of the identity management service;

at the one or more server stations, accepting, from the terminal, an indicator of a condition to be met before the annotation is provided to the third party;

at the one or more server stations, transmitting the annotation to the third party, or agent thereof, based up on the condition.

8. A method of providing a report of information, relating to an individual and stored on a data source used to facilitate trust between parties to a transaction involving the individual, comprising:

from at least a network server, transmitting a form with fields for obtaining identifying information, identifying said individual, to a client terminal;

receiving at at least a network server from said client terminal, identifying information associated with said form fields, said identifying information substantially uniquely identifying said individual;

at at least a network server, authenticating a requester at said client terminal to confirm that said requester is said individual;

at at least a network server, querying at least the data source providing personal information to retrieve retrieved records pertaining to said identifying information and retrieving records;

generating at at least a network server, a report including data derived from said retrieved records;

said step of generating including formatting a web page to include a header showing categories of information in said web page with links to said information;

and further include lists of criteria, used in said step of querying, used to retrieve the records, said lists varying depending on the category of information to which said list corresponds.

9. A method as in claim 8, wherein records are grouped by said categories in said web page and each of said lists of criteria is located adjacent a corresponding group.

10. A method as in claim 8, wherein records are grouped by said categories in said web page and wherein, adjacent each group, is an explanation or a link thereto, describing the nature of the records.

11. A method as in claim 10, wherein said explanation includes an FAQ.

12. A method as in claim 10, wherein said explanation includes an explanation of why data may be missing from the report.

13. A method as in claim 8, wherein records are grouped by said categories in said web page and adjacent each of said groups is a list of data sources from which said records were obtained.

14. A method of providing a report of information, relating to an individual and stored on the data source used to facilitate trust between parties to a transaction involving the individual, comprising:

from at least a network server, transmitting a form with fields for obtaining identifying information, identifying said individual, to a client terminal;

receiving at at least a network server from said client terminal, identifying information associated with said form fields, said identifying information substantially uniquely identifying said individual;

at at least a network server, authenticating a requester at said client terminal to confirm that said requester is said individual;

at at least a network server, querying at least the data source providing personal information to retrieve retrieved records pertaining to said identifying information and retrieving records;

said step of querying including submitting various queries whose results may or may not be included in the report depending on the results of the querying;

selecting certain records to include in a report based on results of said step of querying;

generating at at least a network server, a report including data derived from said retrieved records;

said step of generating including formatting a web page to include a list of queries used to generate records selected in said step of selecting.

15. A method as in claim 14, further comprising transmitting said report to a client terminal.

16. A method as in claim 14, wherein said list of queries indicates a number of records retrieved based on each of the queries appearing in said list.

17. A method as in claim 14, wherein said background information includes address data, real estate records, and name data.

18. A method as in claim 14, wherein said list of queries includes social security number and at least one format of name and address of said individual.

19. A method as in claim 14, wherein said list is shown as an expanded list and can be collapsed by user-selection of a web control or link, a collapsed representation of the list including a control to permit display of the complete list and a summary of the list in the form of at least a total count or records in said list.

20. A method of providing a report of information, relating to an individual and stored on a data source used to facilitate trust between parties to a transaction involving the individual, comprising:

from at least a network server, transmitting a form with fields for obtaining identifying information, identifying an individual, to a client terminal;

receiving at at least a network server from said client terminal, identifying information associated with said form fields, said identifying information substantially uniquely identifying an individual person;

at at least a network server, creating a customer profile corresponding to a customer and corresponding to said identifying information;

at at least a network server, querying at least two data sources containing publicly-available information corresponding to said identifying information;

retrieving as a result of said querying, at least two pieces of information relating to a same event, person, or thing;

generating a report containing both of said at least two pieces;

transmitting said report to a client terminal;

said report being arranged to indicate discrepancies at least by displaying both of said two pieces of information.

21. A method as in claim 20, wherein said step of generating further comprises including in said report at least one instruction for repairing a discrepancy between said at least two pieces of information.

22. A method as in claim 21, wherein said step of generating further comprises including in said report at least one computer decodable link to a control or

web site with information about how to respond to said discrepancy between said at least two pieces of information.

23. A method as in claim 20, wherein said step of generating includes identifying said at least two pieces of information as relating to a same event, person, or thing and formatting said report to juxtapose, in a special manner, said two pieces of information, whereby a user is easily able to understand a discrepancy in data housed at separate data sources.

24. A method as in claim 20, wherein said step of generating includes identifying said at least two pieces of information as relating to a same event, person, or thing and including an indication of a result of said identifying in said report, whereby a user is easily able to understand a discrepancy in data housed at separate data sources.

25. A method of providing a report of information, relating to an individual and stored on a data source used to facilitate trust between parties to a transaction involving the individual, comprising:

from at least a network server, transmitting a form with fields for obtaining identifying information, identifying an individual, to a client terminal;

receiving at at least a network server from said client terminal, identifying information associated with said form fields, said identifying information substantially uniquely identifying an individual person;

at at least a network server, querying, based at least in part on said information an aggregator data source containing records from multiple primary data sources including at least state and federal records pertaining to various persons, events, and/or things and retrieving a resulting set of records;

at at least a network server, querying one of said multiple primary data sources and retrieving at least one record that pertains to a same one of said various persons, events, and/or things;

generating a report containing both of said at least one record and said resulting set of records such that said at least one record can be compared to one pertaining to said same one of said various persons, events, and/or things, by a user, to determine if discrepancies exist;

transmitting said report to a client terminal.

26. A method as in claim 25, wherein said step of generating further comprises including in said report at least one instruction for repairing a discrepancy between two pieces of information.

27. A method as in claim 26, wherein said step of generating further comprises including in said report at least one computer decodable link to a control or web site with information about how to respond to said discrepancy between two pieces of information.

28. A method as in claim 25, wherein said step of generating includes identifying records retrieved in said first and second steps of retrieving that correspond to a same person, event, and/or thing and formatting said report responsively to a result of said identifying.

29. A method as in claim 28, wherein said step of formatting includes aligning discrepant portions of said records in adjacent positions in said report.

30. A method of providing a report of information, relating to an individual and stored on a data source used to facilitate trust between parties to a transaction involving the individual, comprising:

generating a user interface to allow customers to obtain personal information about themselves that are stored at publicly-available data sources;

said user interface permitting customers of a service to enter identifying information and authenticating information;

at at least a network server, authenticating a user and storing corresponding identifying information pertaining to said user;

at at least a network server, querying, based on said identifying information, an aggregator data source containing records derived from a primary data source and retrieving aggregator records resulting from said first step of querying;

at at least a network server, querying, based on said identifying information, said primary data source and retrieving primary records resulting from said second step of querying;

generating a report containing said primary and aggregator records in a format that allows comparison by a user;

at least one of said primary and aggregator records pertaining to a same person, event, and/or thing and containing redundant information unless a discrepancy between at least a corresponding portion of each of said primary and aggregator records exists.

31. A method as in claim 30, wherein said step of generating further comprises including in said report at least one instruction for repairing a discrepancy between two pieces of information.

32. A method as in claim 31, wherein said step of generating further comprises including in said report at least one computer decodable link to a control or web site with information about how to respond to a discrepancy between two pieces of information in said report.

33. A method as in claim 32, wherein said decodable link to a control or web site with information is provided in said report adjacent records containing information from both primary and aggregator records that may pertain to a same person, event, and/or thing.

34. A method as in claim 30, wherein said step of generating includes identifying records retrieved in said first and second steps of retrieving that correspond to a same person, event, and/or thing and formatting said report responsively to a result of said identifying.

35. A method as in claim 34, wherein said step of formatting includes aligning discrepant portions of said records in adjacent positions in said report.

36. A method of providing a report of information, relating to an individual and stored on a data source used to facilitate trust between parties to a transaction involving the individual, comprising:

from at least a network server, transmitting a form with fields for obtaining identifying information, identifying said individual, to a client terminal;

receiving at at least a network server from said client terminal, identifying information associated with said form fields, said identifying information substantially uniquely identifying said individual;

at at least a network server, authenticating a requester at said client terminal to confirm that said requester is said individual;

at at least a network server, performing a process including querying the data source, said process resulting in a final set of records resulting from said querying and pertaining to said identifying information;

said process being such that said final set includes records satisfying a strict matching criterion and records not satisfying said strict matching criterion, but satisfying a less strict matching criterion, when records in said data source include less than a predetermined number satisfying said strict matching criterion, but includes only records satisfying said strict matching criterion when records in said data source include at least a predetermined number satisfying said strict matching criterion;

generating at at least a network server, a report including data from said final set of records.

37. A method as in claim 36, wherein said process includes querying said data source with a first strict criterion and counting a number of records retrieved then querying said data source with a second less strict criterion when said number of records is less than a predetermined number.

38. A method as in claim 36, wherein all records in said final set correspond to a result of a same query, whereby no records are arbitrarily excluded from said final set.

39. A method as in claim 36, wherein said strict matching criterion includes a full address and said less strict matching criterion includes only a partial address.

40. A method as in claim 39, wherein said partial address has no street portion of an address.

41. A method of providing a report of information, relating to an individual and stored on a data source used to facilitate trust between parties to a transaction involving the individual, comprising:

from at least a network server, transmitting a form with fields for obtaining identifying information, identifying said individual, to a client terminal;

receiving at at least a network server from said client terminal, identifying information associated with said form fields, said identifying information substantially uniquely identifying said individual;

at at least a network server, authenticating a requester at said client terminal to confirm that said requester is said individual;

at at least a network server, querying the data source and retrieving a final set of records resulting from said querying and pertaining to said identifying information;

said final set including records corresponding to a result of a narrow query and a broad query when the number of records in said data source satisfying said broad query is less than a predetermined number;

generating at at least a network server, a report including data from said final set of records;

transmitting said report to a client terminal.

42. A method as in claim 41, wherein said report includes a list of criteria satisfied by records reported therein such that said list includes, correspondingly, a specification of both said narrow and broad queries or only a specification of said narrow query.

43. A method as in claim 41, wherein said step of querying includes iteratively querying said data source until said predetermined number is reached.

44. A A method of providing a report of information, relating to an individual and stored on a data source used to facilitate trust between parties to a transaction involving the individual, comprising:

from at least a network server, transmitting a form with fields for obtaining identifying information, identifying said individual, to a client terminal;

receiving at at least a network server from said client terminal, identifying information associated with said form fields, said identifying information substantially uniquely identifying said individual;

at at least a network server, authenticating a requester at said client terminal to confirm that said requester is said individual;

at at least a network server, querying the data source and retrieving a final set of records resulting from said querying and pertaining to said identifying information;

determining if a predetermined number of records has been obtained;

at least one of querying an additional data source or querying, based on a less strict query, a same data source when less than said predetermined number is determined;

generating at at least a network server, a report including data from said final set of records;

transmitting said report to a client terminal.

45. A method as in claim 44, wherein said report includes a list of criteria satisfied by records reported therein such that said list includes, correspondingly, a specification of both said narrow and broad queries or only a specification of said narrow query.

46. A method as in claim 44, wherein said report includes a list of data sources accessed to generate said report.

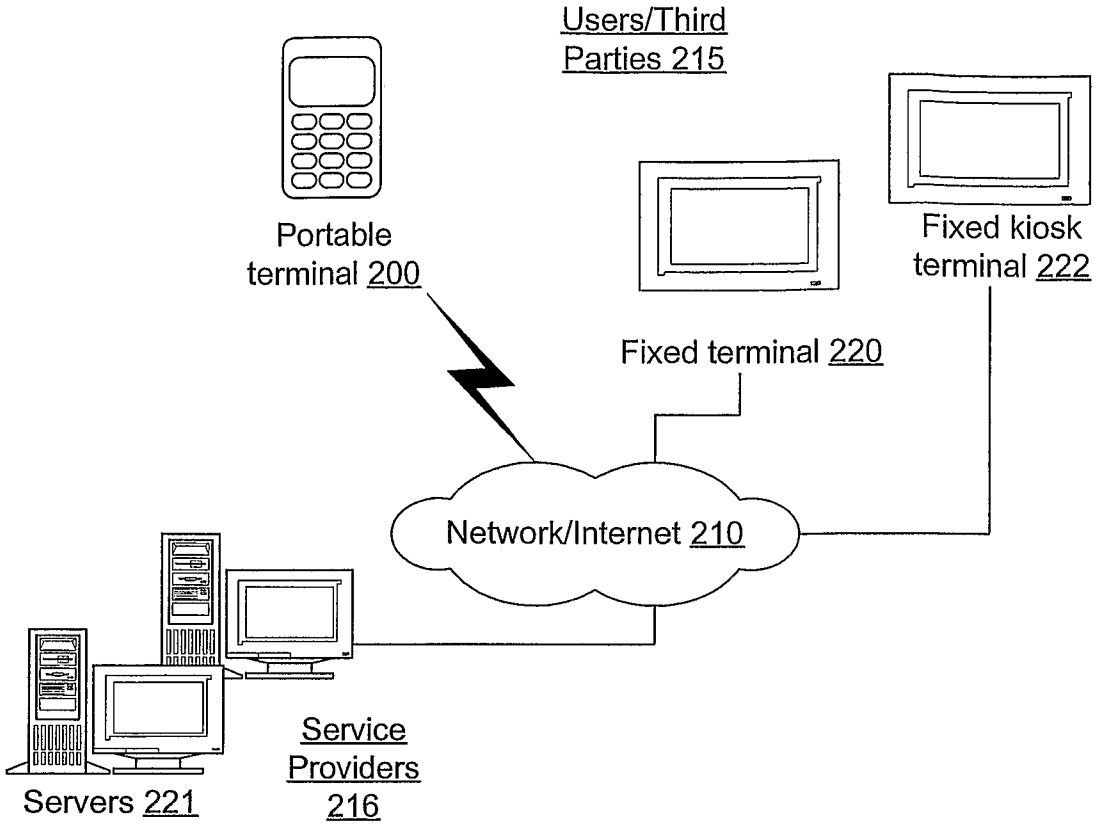

Users/Third Parties 215
Portable terminal 200
Fixed kiosk terminal 222
Fixed terminal 220
Network/Internet 210
Service Providers 216
Servers 221

Fig. 1

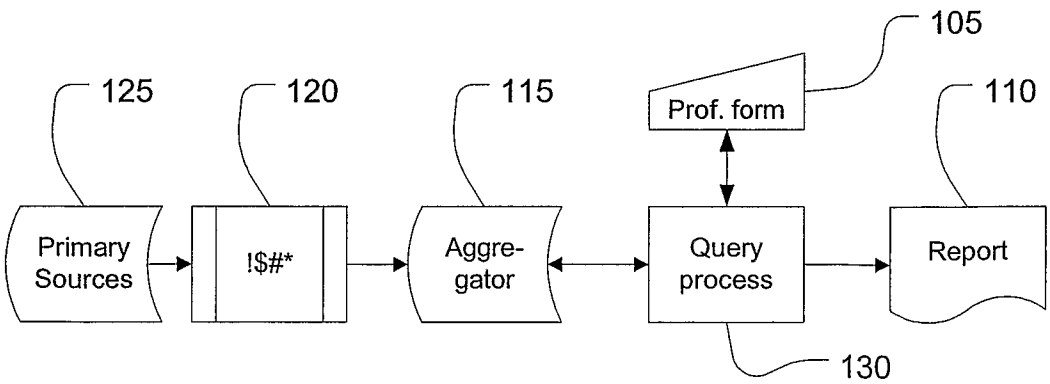

125
120
115
105
110
Prof. form
Primary Sources
!$#*
Aggre-gator
Query process
Report
130

Fig. 2A

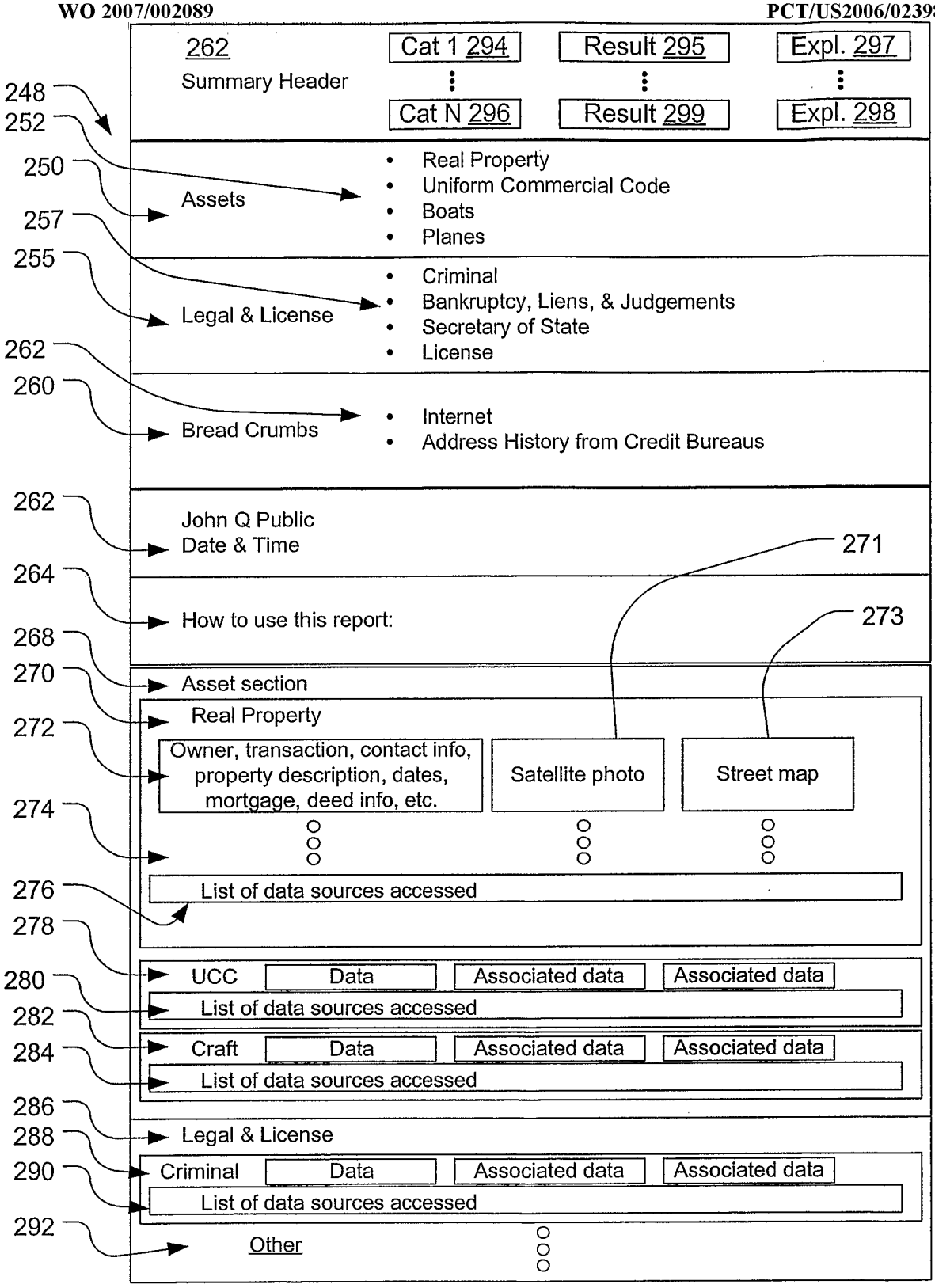

262
Summary Header
Cat 1 294
Cat N 296
Result 295
Result 299
Expl. 297
Expl. 298
248
252
250
257
255
262
260
262
264
268
270
272
274
276
278
280
282
284
286
288
290
292
Assets
Real Property
Uniform Commercial Code
Boats
Planes
Legal & License
Criminal
Bankruptcy, Liens, & Judgements
Secretary of State
License
Bread Crumbs
Internet
Address History from Credit Bureaus
John Q Public
Date & Time
How to use this report:
271
273
Asset section
Real Property
Owner, transaction, contact info, property description, dates, mortgage, deed info, etc.
Satellite photo
Street map
List of data sources accessed
UCC
Data
Associated data
Associated data
List of data sources accessed
Craft
Data
Associated data
Associated data
List of data sources accessed
Legal & License
Criminal
Data
Associated data
Associated data
List of data sources accessed
Other

Fig. 2B

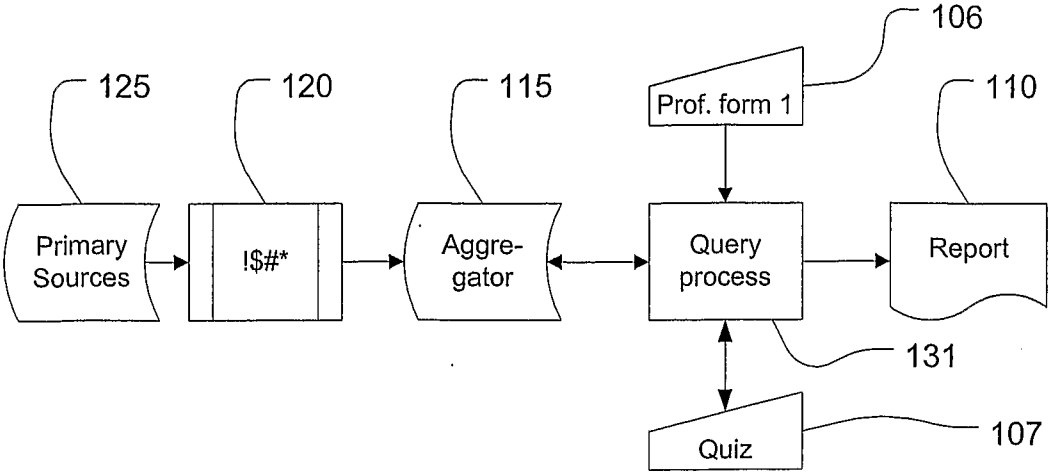

106
125
120
115
Prof. form 1
110
Primary Sources
!$#*
Aggre-gator
Query process
Report
131
Quiz
107

Fig. 3

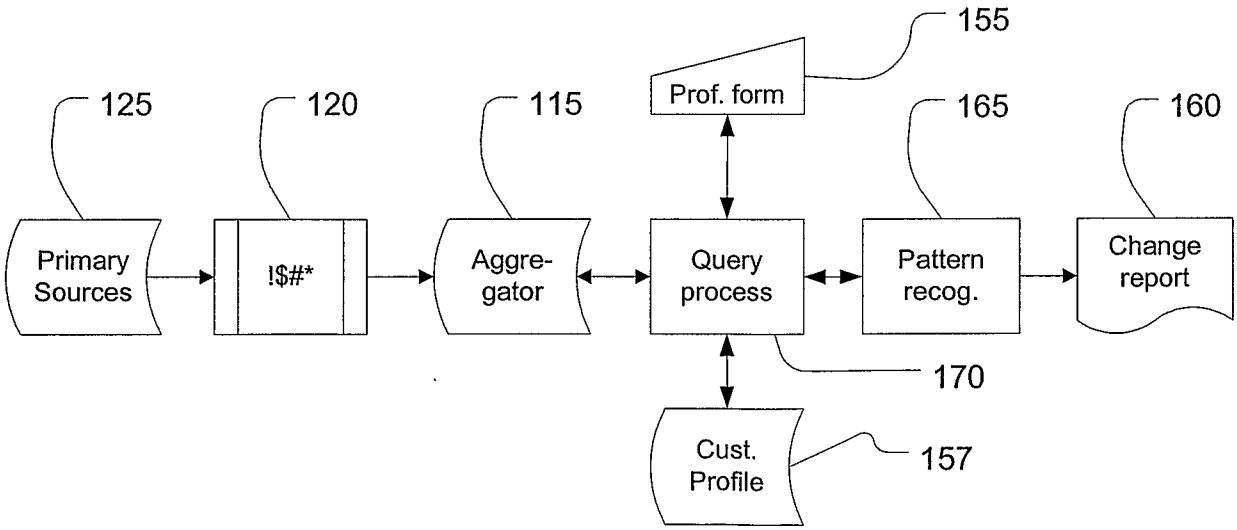

155
125
120
115
Prof. form
165
160
Primary Sources
!$#*
Aggre-gator
Query process
Pattern recog.
Change report
170
Cust. Profile
157

Fig. 4

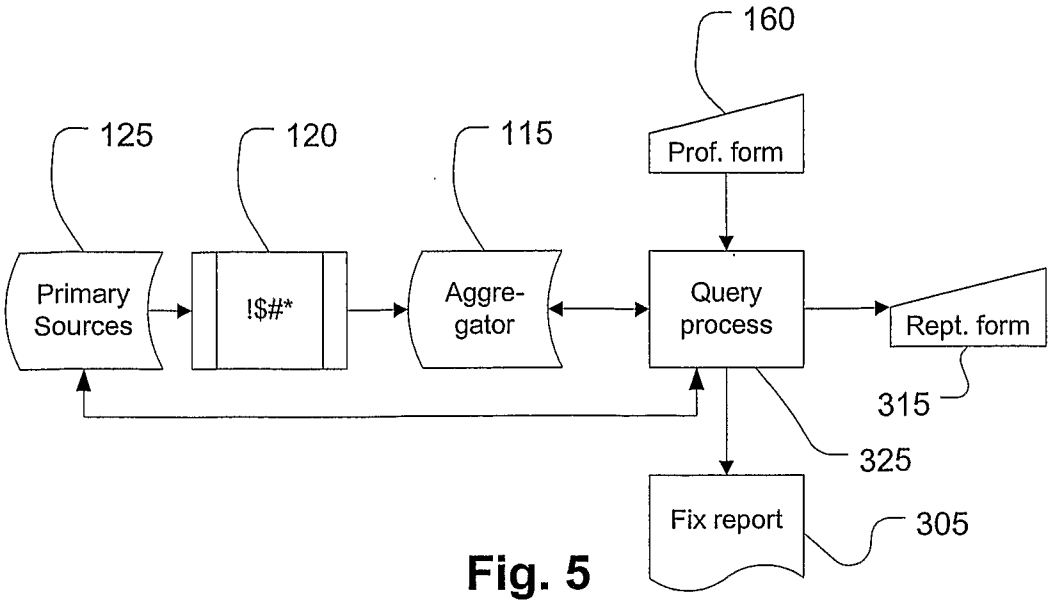

160
125
120
115
Prof. form
Primary Sources
!$#*
Aggre-gator
Query process
Rept. form
315
325
Fix report
305

Fig. 5

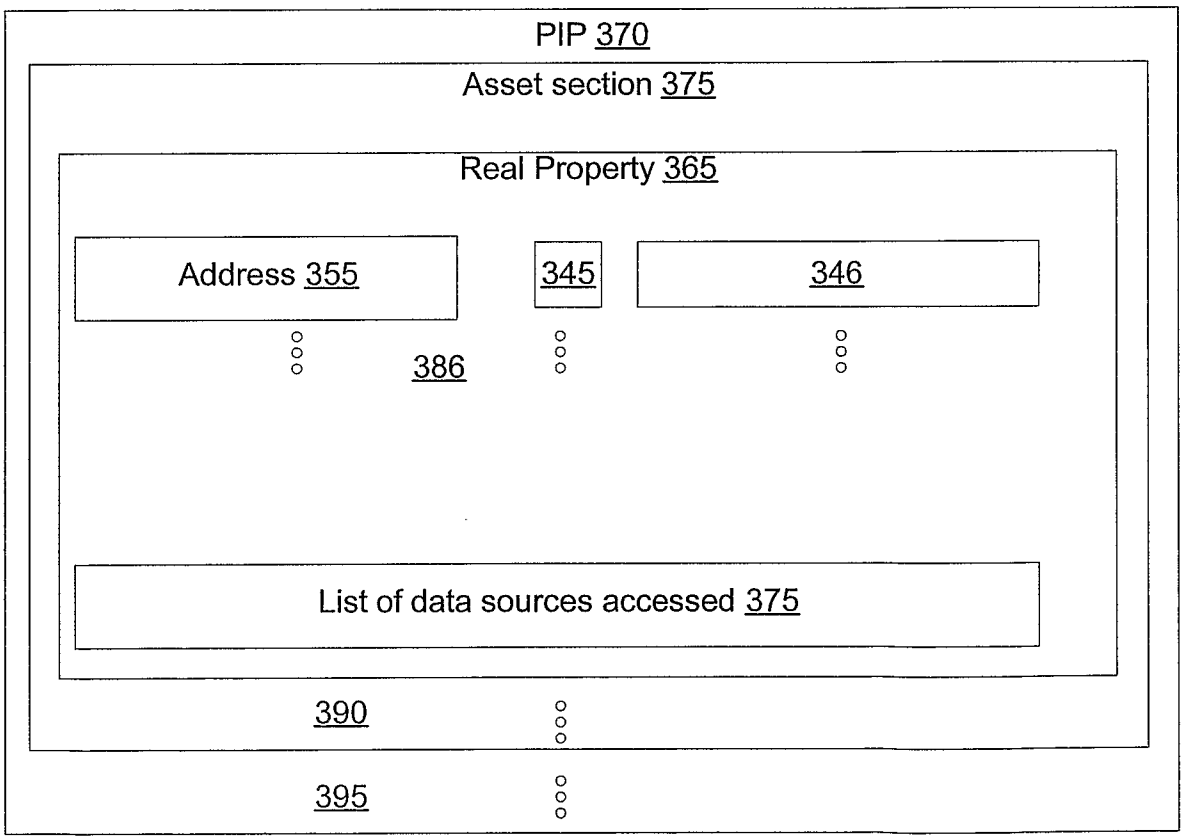

PIP 370
Asset section 375
Real Property 365
Address 355
345
346
386
List of data sources accessed 375
390
395

Fig. 6

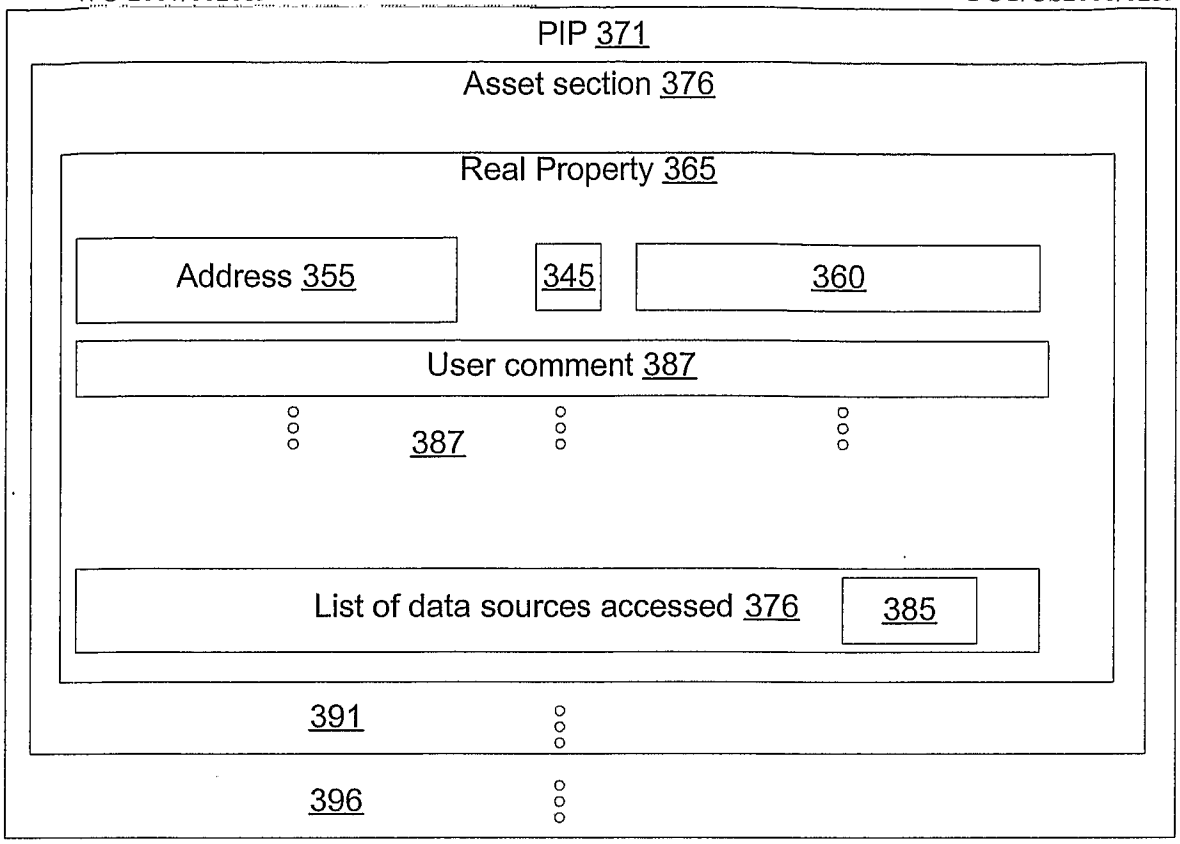

PIP 371
Asset section 376
Real Property 365
Address 355
345
360
User comment 387
387
List of data sources accessed 376
385
391
396

Fig. 7

1234 Dim Sum Lane, Mauborgne, LA

Assessment Record - County of: MONTGOMERY, MD

Owner Contact

Owner:	John Q Public
Other owners:	
Contact phone:	222-555-3333
Mailing address:	1234 Dim Sum Lane, Mauborgne, LA 77777
Company:	

Physical details

Property type:	SINGLE FAMILY RESIDENCE/TOWNHOUSE (10)
Cooling/heating:	AC.SPLIT SYSTEM(T)/HOT AIR (HA0)
Roof:	COMPOSITION SHINGLE(15)
Exterior walls:	BRICK(BRI)
Year built:	1956
Construction Quality:	GOOD (7)
Square ft/:lot size (d x w):	3506/11443 (x)

Pool:	Fireplace:	View:	Garage:
	Y		B00(ATTACHED CARPORT sq ft)

Stories:	Units:	Rooms:	Beds:	Baths:
1				3.0

Sales Information

Sales date:	20030611
Document Number:	
Last Sale $:	$649000
Loan amount (1st/2nd):	519200/
Lender:	ABN AMRO MTG GRP INC
Interest rate/Loan type:	/CONVENTIONAL(C)
Title ins.:	FIDELITY NAT'L TITLE INS CO/NY
Deed type:	GRANT DEED(G)
Previous transaction (Doc #):	19770223
Year sold to state:	

Tax Assessments

Tax amount:	$6143
Total assessed $:	$577630
Percent improved:	%
Homeowner exempt:	

Legal Definitions

Parcel:	GN62 0000 0000 0001 0021 07000000619392
Description (Block-Lot):	Nirvana
Zoning:	R90
Census tract:	888.26
Municipality:	
Maps:	Map page (old/new): GN56/GN56 Map grid (new): X/Y coord: /38978747

Fig. 8

Data sources for Real Property Areas

AK

AK Anchorage: TaxRoll	AK Fairbanks North Star Borough: TaxRoll	AK Juneau Borough: TaxRoll	AK Kenai: TaxRoll	AK Kenai Peninsula: TaxRoll	AK Ketchikan Gateway Borough: TaxRoll
AK Matanuska-Susitna (Palmer): TaxRoll	AK Matanuska-Susitna Borough: TaxRoll				

AL

AL Autauga: TaxRoll	AL Baldwin: TaxRoll	AL Barbour: TaxRoll	AL Blount: TaxRoll	AL Calhoun: TaxRoll	AL Chilton: TaxRoll
AL Choctaw: TaxRoll	AL Colbert: TaxRoll	AL Cullman: TaxRoll	AL Dale: TaxRoll	AL Dallas: TaxRoll	AL Dekalb: TaxRoll
AL Elmore: TaxRoll	AL Etowah: TaxRoll	AL Fayette: TaxRoll	AL Franklin: TaxRoll	AL Hale: TaxRoll	AL Henry: TaxRoll
AL Jackson: TaxRoll	AL Jefferson: Deeds & Tax Roll	AL Lauderdale: TaxRoll	AL Lawrence: TaxRoll	AL Lee: TaxRoll	AL Limestone: TaxRoll
AL Macon: TaxRoll	AL Marshall: TaxRoll	AL Mobile: TaxRoll	AL Montgomery: TaxRoll	AL Morgan: TaxRoll	AL Randolph: TaxRoll
AL Russell: TaxRoll	AL Shelby: TaxRoll	AL Talladega: TaxRoll	AL Tallapoosa: TaxRoll	AL Tuscaloosa: TaxRoll	AL Walker: TaxRoll
AL Wilcox: TaxRoll					

AR

AR Baxter: TaxRoll	AR Benton: TaxRoll	AR Boone: TaxRoll	AR Craighead: TaxRoll	AR Crittenden: TaxRoll	AR Faulkner: TaxRoll
AR Garland: TaxRoll	AR Greene: TaxRoll	AR Hot Spring: TaxRoll	AR Independence: TaxRoll	AR Jefferson: TaxRoll	AR Lonoke: TaxRoll
AR Miller: TaxRoll	AR Ouachita: TaxRoll	AR Phillips: TaxRoll	AR Poinsett: TaxRoll	AR Pope: TaxRoll	AR Pulaski: TaxRoll
AR Saline: TaxRoll	AR Sebastian: TaxRoll	AR St. Francis: TaxRoll	AR White: TaxRoll		

AZ

AZ Apache: Deeds & Tax Roll	AZ Cochise: Deeds & Tax Roll	AZ Coconino: Deeds & Tax Roll	AZ Gila: Deeds & Tax Roll	AZ Graham: Deeds & Tax Roll	AZ Greenlee: TaxRoll

Fig. 9

IF YOU THINK YOU HAVE BEEN THE VICTIM OF IDENTITY THEFT

The Federal Trade Commission (FTC) recommends taking the following actions:

1. Place a Fraud Alert on your credit file with one of the three major credit bureaus, Equifax, Experian, and TransUnion. Keep a log of every call you make, and note the date, time, length of conversation, and name of the person with whom you spoke.

Equifax

1-888-766-0008

Equifax Credit Information Services, Inc

P.O. Box 740241

Atlanta, GA 30374

Experian

1-888 397 374

P.O. Box 2104

Fig. 10

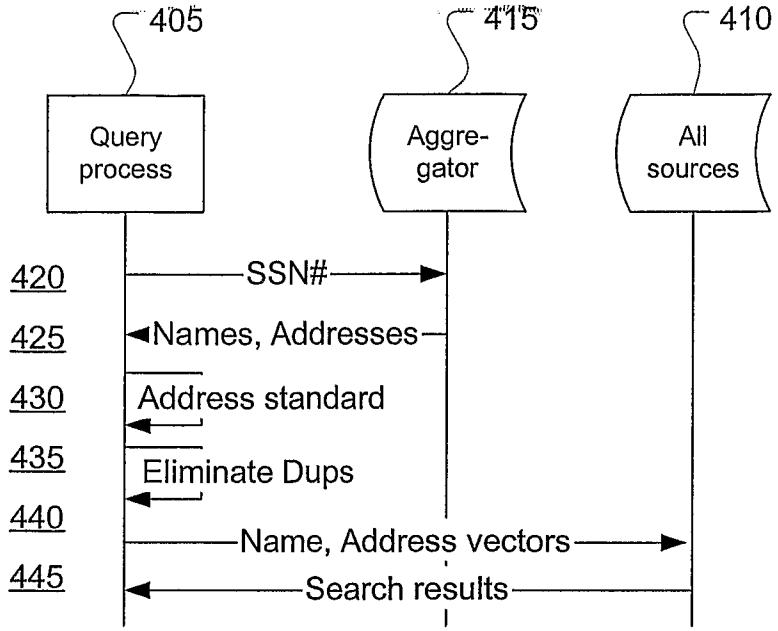

405
415
410
Query process
Aggre-gator
All sources
420
SSN#
425
Names, Addresses
430
Address standard
435
Eliminate Dups
440
Name, Address vectors
445
Search results

Fig. 11

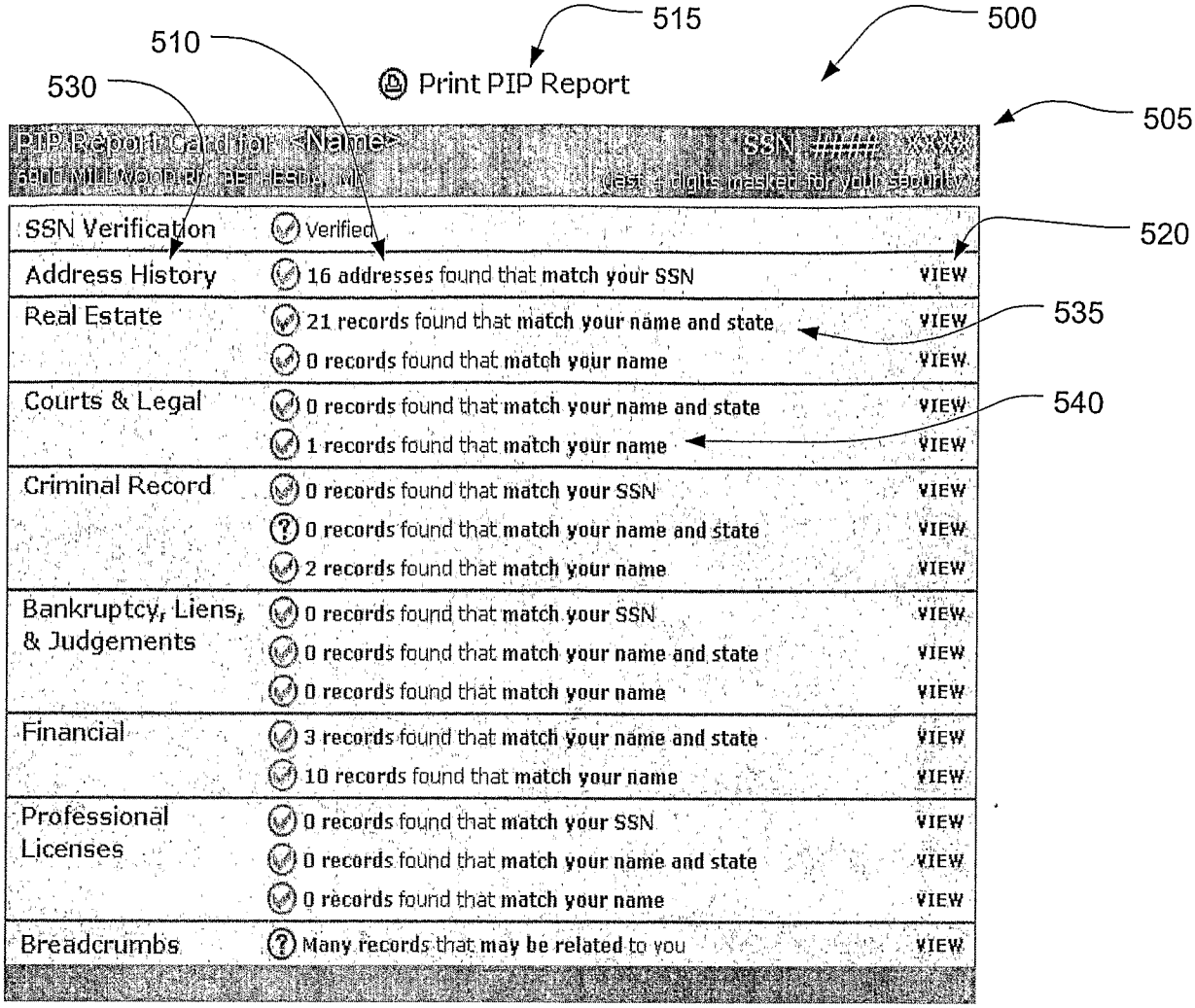

515
500
510
530
Print PIP Report
505
PIP Report Card for <Name>
SSN
520
SSN Verification
Verified
Address History
16 addresses found that match your SSN
VIEW
Real Estate
21 records found that match your name and state
VIEW
535
0 records found that match your name
VIEW
Courts & Legal
0 records found that match your name and state
VIEW
540
1 records found that match your name
VIEW
Criminal Record
0 records found that match your SSN
VIEW
0 records found that match your name and state
VIEW
2 records found that match your name
VIEW
Bankruptcy, Liens, & Judgements
0 records found that match your SSN
VIEW
0 records found that match your name and state
VIEW
0 records found that match your name
VIEW
Financial
3 records found that match your name and state
VIEW
10 records found that match your name
VIEW
Professional Licenses
0 records found that match your SSN
VIEW
0 records found that match your name and state
VIEW
0 records found that match your name
VIEW
Breadcrumbs
Many records that may be related to you
VIEW

Fig. 12

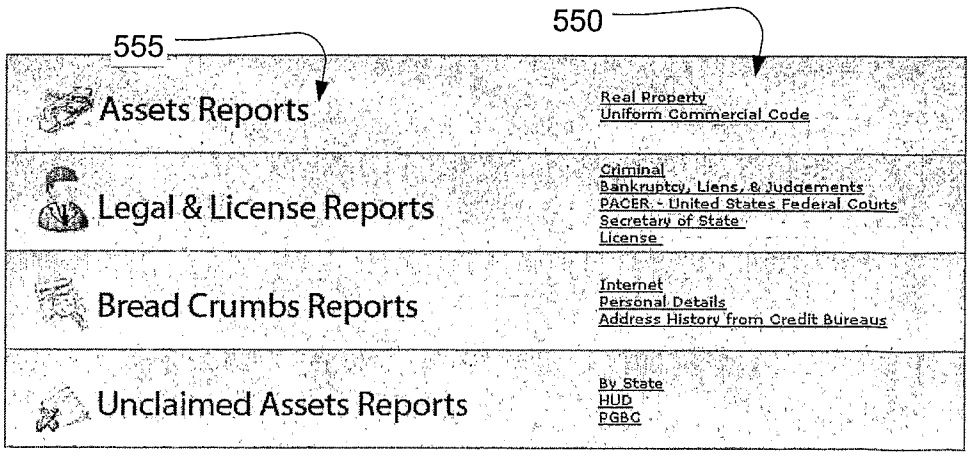

555
550
Assets Reports
Real Property
Uniform Commercial Code
Legal & License Reports
Criminal
Bankruptcy, Liens, & Judgements
PACER - United States Federal Courts
Secretary of State
License
Bread Crumbs Reports
Internet
Personal Details
Address History from Credit Bureaus
Unclaimed Assets Reports
By State
HUD
PGBC

Fig. 13

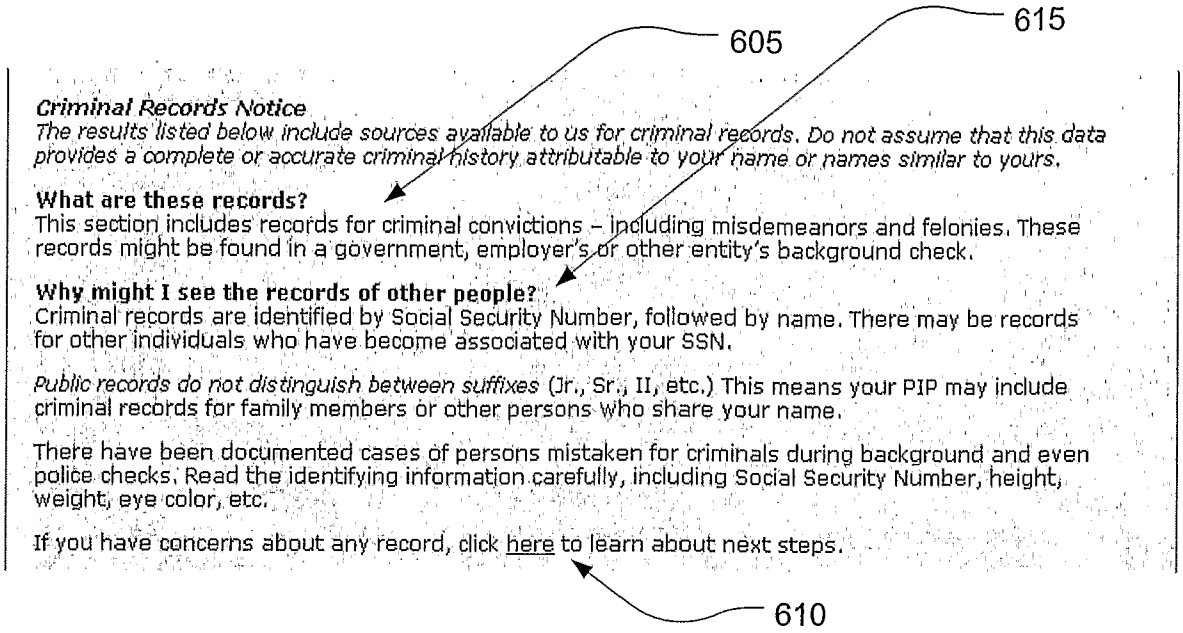

605
615
Criminal Records Notice
The results listed below include sources available to us for criminal records. Do not assume that this data provides a complete or accurate criminal history attributable to your name or names similar to yours.
What are these records?
This section includes records for criminal convictions – including misdemeanors and felonies. These records might be found in a government, employer's or other entity's background check.
Why might I see the records of other people?
Criminal records are identified by Social Security Number, followed by name. There may be records for other individuals who have become associated with your SSN.
Public records do not distinguish between suffixes (Jr., Sr., II, etc.) This means your PIP may include criminal records for family members or other persons who share your name.
There have been documented cases of persons mistaken for criminals during background and even police checks. Read the identifying information carefully, including Social Security Number, height, weight, eye color, etc.
If you have concerns about any record, click here to learn about next steps.
610

Fig. 14

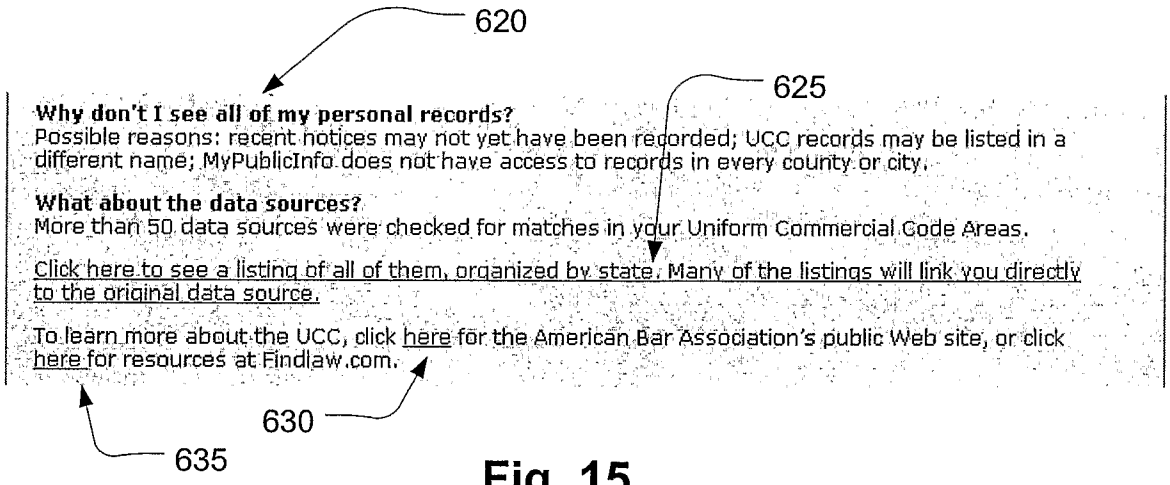

620
625
Why don't I see all of my personal records?
Possible reasons: recent notices may not yet have been recorded; UCC records may be listed in a different name; MyPublicInfo does not have access to records in every county or city.
What about the data sources?
More than 50 data sources were checked for matches in your Uniform Commercial Code Areas.
Click here to see a listing of all of them, organized by state. Many of the listings will link you directly to the original data source.
To learn more about the UCC, click here for the American Bar Association's public Web site, or click here for resources at Findlaw.com.
630
635

Fig. 15

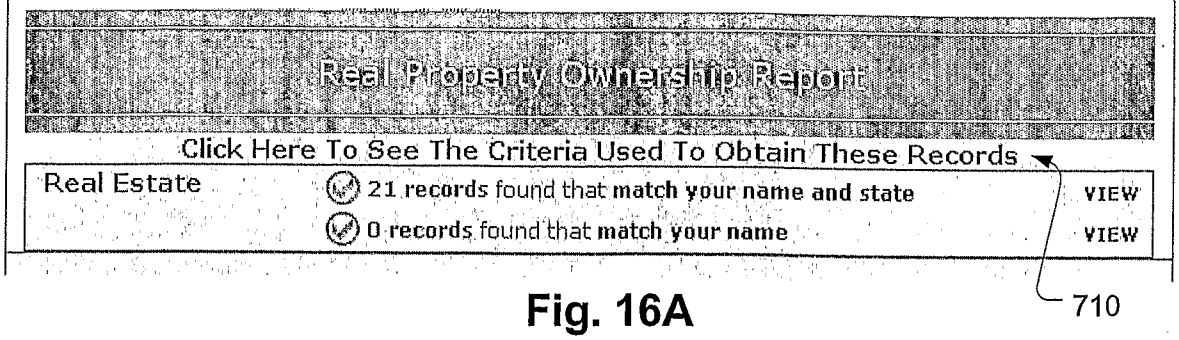


Fig. 16A

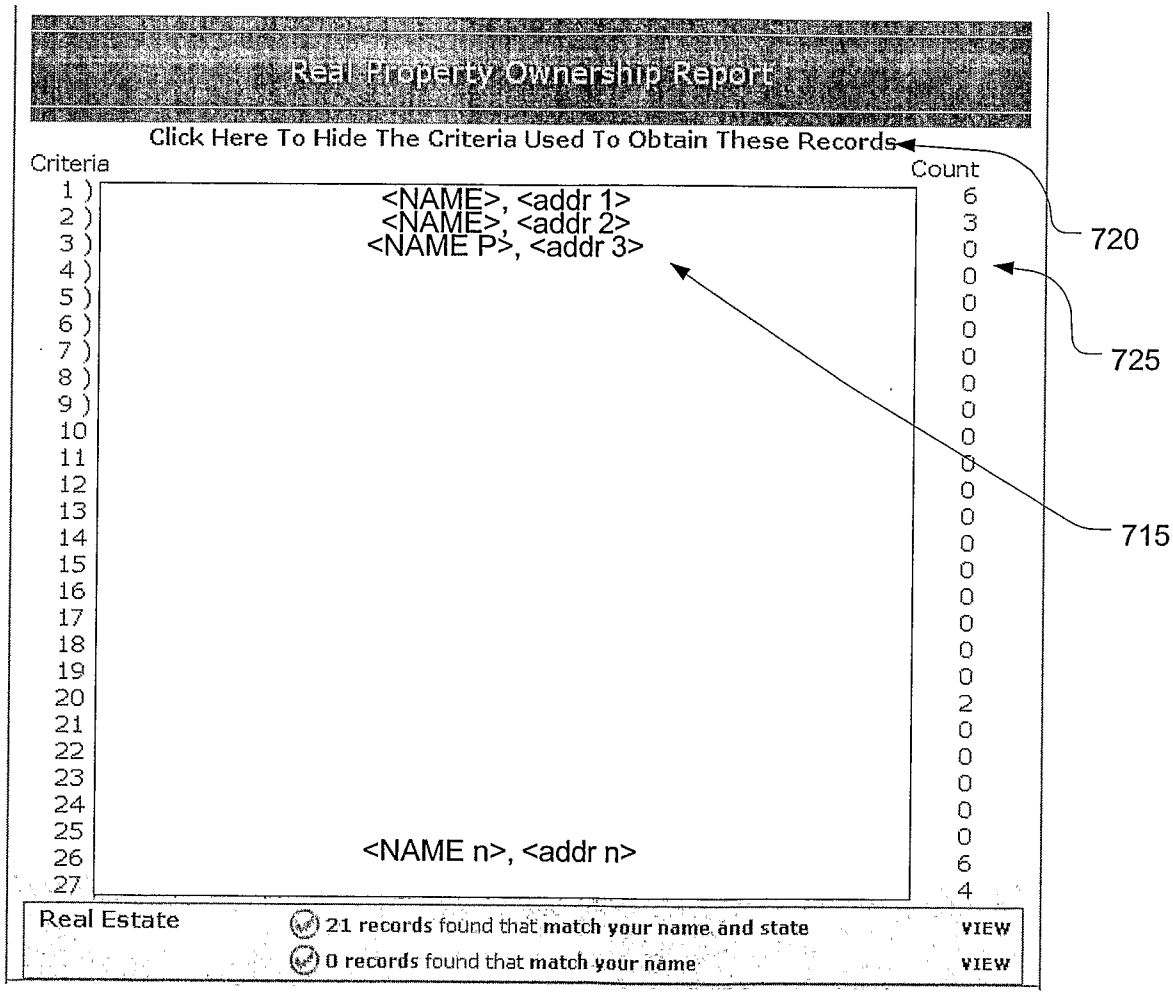


Fig. 16B

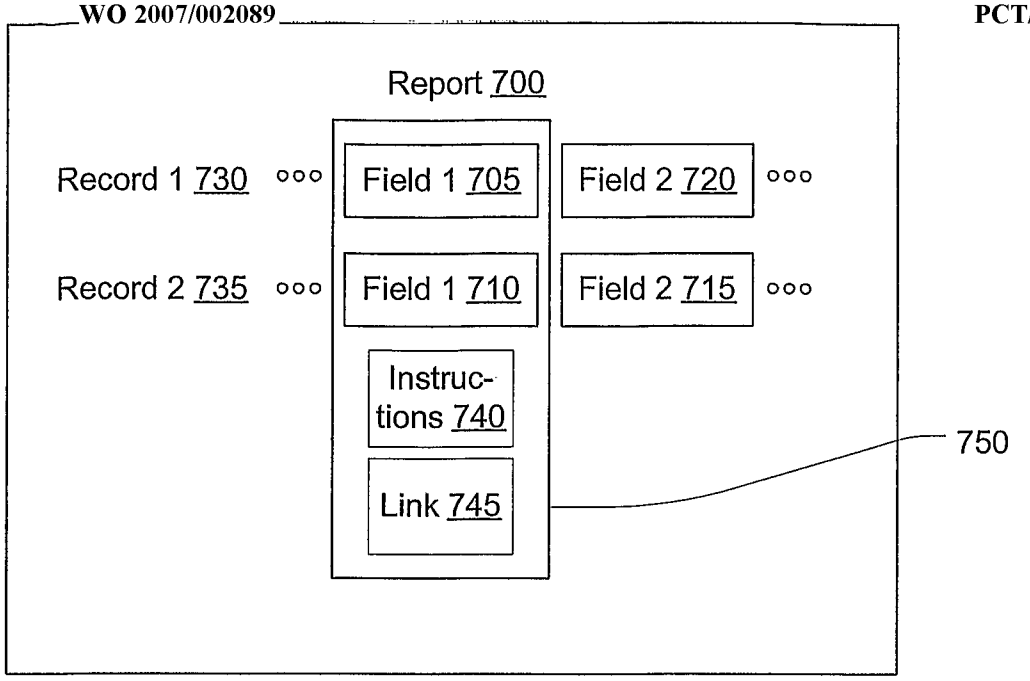

Report 700
Record 1 730
Field 1 705
Field 2 720
Record 2 735
Field 1 710
Field 2 715
Instruc-tions 740
Link 745
750

Fig. 17

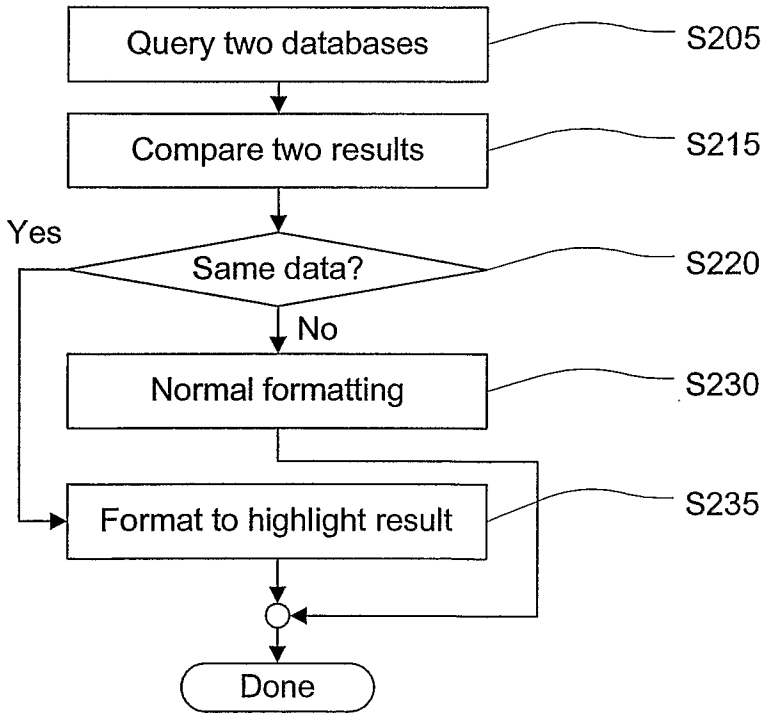

Query two databases
S205
Compare two results
S215
Yes
Same data?
S220
No
Normal formatting
S230
Format to highlight result
S235
Done

Fig. 18

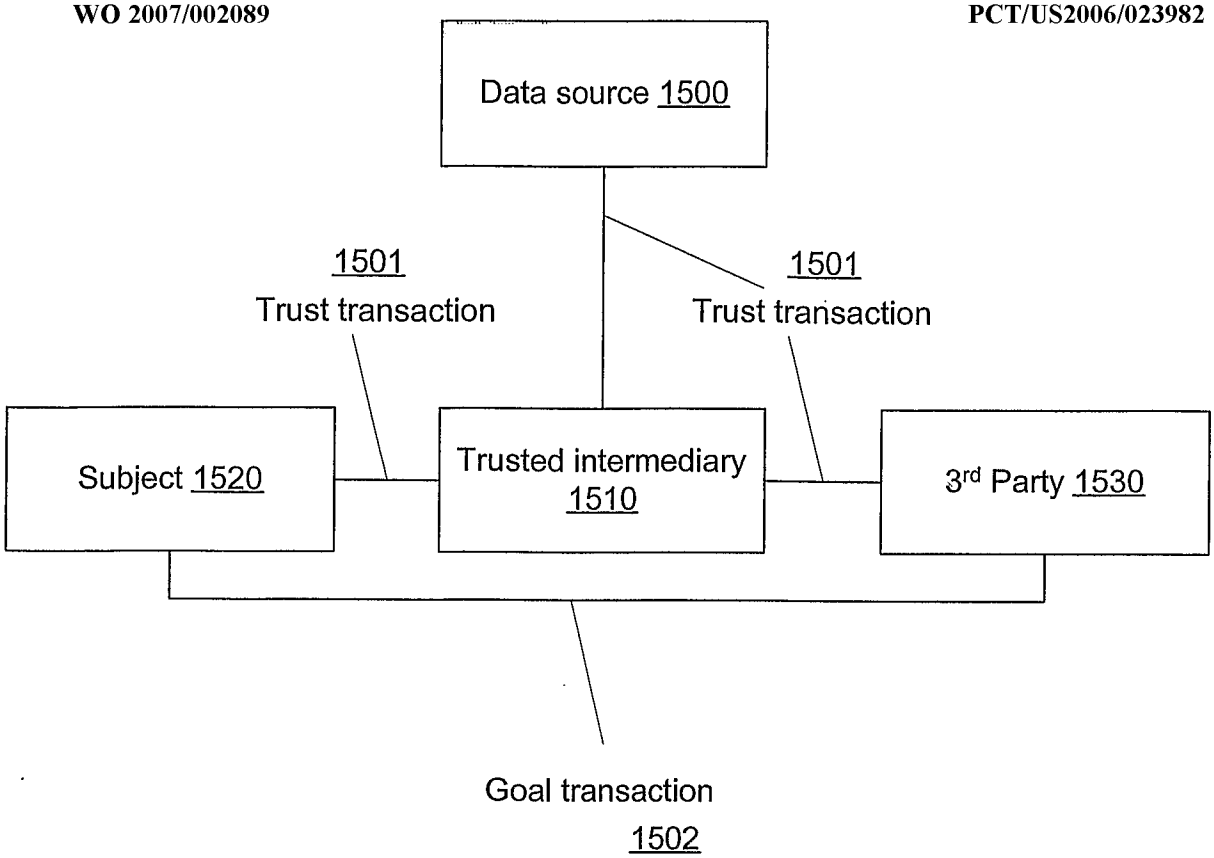

Data source 1500
1501
Trust transaction
1501
Trust transaction
Subject 1520
Trusted intermediary
1510
3rd Party 1530
Goal transaction
1502

Fig. 19