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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 November 2010 (18.11.2010)

PCT

(10) International Publication Number
WO 2010/132492 A2

(51) **International Patent Classification:**
G06F 21/24 (2006.01)

(21) **International Application Number:**
PCT/US20 10/034434

(22) **International Filing Date:**
11 May 2010 (11.05.2010)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
61/177,205 11 May 2009 (11.05.2009) US

(71) **Applicant** *(for all designated States except US):* **EXPERIAN MARKETING SOLUTIONS, INC.** [US/US]; 955 American Lane, Schaumburg, IL 601 73 (US).

(72) **Inventors; and**

(75) **Inventors/Applicants** *(for US only):* **STACK, Brian** [US/US]; 30 Palatine #446, Irvine, CA 92612 (US). LIENTZ, **Andrew** [US/US]; 4288 Revere Place, Culver City, CA 90232 (US). CHAMBERLAIN, **Simon** [AU/AU]; 8 Kerferd Place, Albert Park, Victoria 3206 (AU). ABDOUS, **Yacine** [US/US]; 20946 Halldale Ave., Torrance, CA 90501 (US). KAHN, **Ray** [US/US]; 2 Medici, Aliso Viejo, CA 92656 (US).

(74) **Agent:** ALTMAN, **Daniel** E.; Knobbe Martens Olson & Bear, LLP, 2040 Main Street, Fourteenth Floor, Irvine, CA 92614 (US).

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

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

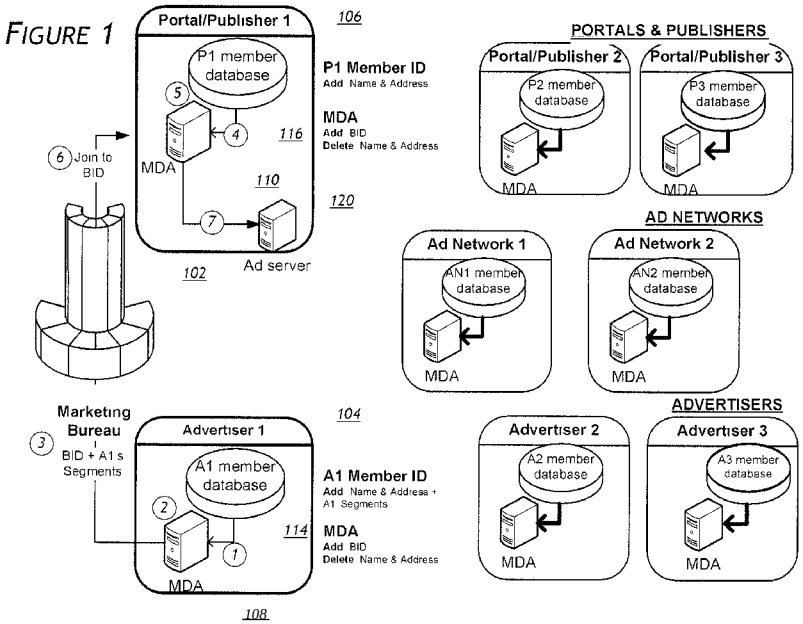
Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.1 7(H))*

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR PROVIDING ANONYMIZED USER PROFILE DATA

FIGURE 1



(57) Abstract: Embodiments facilitate confidential and secure sharing of anonymous user profile data to improve the delivery of customized content. Embodiments of the invention provide a data appliance to an entity such as a business to convert profile data about the business's customers into anonymous identifiers. A similar data appliance is provided to a content provider in one embodiment to generate identifiers for its user profile data. Because the anonymous identifiers are generated with the same anonymization method, identical identifiers are likely generated from profile data of the same users. Therefore, the identifiers can be used to anonymously match the customers of the business to the users of the content provider. Therefore, data can be shared to improve customized content such as advertisements that the business wishes to place with the content provider without requiring the business to disclose customer data in an unencrypted form, and any non-matched data can remain confidential.

WO 2010/132492 A2

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(gJ)*

EXP.325VPC PATENT

SYSTEMS AND METHODS FOR PROVIDING ANONYMIZED USER PROFILE DATA

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of priority from United States Provisional Patent Application No. 61/177,205 filed on May 11, 2009, entitled "Systems and Methods for Providing Anonymized Marketing Information," the entire contents of which are hereby incorporated herein by reference in their entirety. All publications and patent applications mentioned in this specification are herein incorporated by reference in their entirety to the same extent as if each individual publication or patent application was specifically and individually indicated to be incorporated by reference.

BACKGROUND

Field

[000 2] This disclosure relates in general to computer data processing, and in particular to computer based systems and methods for providing anonymized user profile data.

Description of the Related Art

[0003] In the online environment, the effective delivery of customized content is dependent on the quality of known data about the intended consumers of such content. For example, the effectiveness of an advertisement ("ad") is enhanced when it is delivered to a person whose attributes and/or other recorded past actions indicate possible interest in the content of the ad. While user profile data may be used to customize the delivered content, the sharing of such data is hindered by reluctance among entities that hold such data out of competitive and privacy concerns. For example, while an advertiser may benefit from improved ad

customization as a result of sharing information about its customers with a content publisher from which it wishes to purchase ads, the advertiser is typically reluctant to share such data.

SUMMARY OF THE DISCLOSURE

[0004] Embodiments of the disclosure are directed to computer based systems and methods for sharing user profile data in an anonymized manner. Embodiments facilitate confidential and secure sharing of de-personalized and/or anonymous customer profile data among entities to improve the delivery of customized content. For example, embodiments of the invention provide a data appliance to an entity such as a business to convert profile data about the business's customers into anonymous identifiers. A similar data appliance is provided to a content provider in one embodiment to generate identifiers for its user profile data. A central server connected to the data appliances facilitate the sharing of the anonymous identifiers across data networks. In one embodiment, because the anonymous identifiers are generated with the same anonymization method, identical identifiers are likely generated from profile data of the same users. Therefore, the identifiers can be used to anonymously match the customers of the business to the users of the content provider. As such, the matched data can be shared to improve the delivery of customized content such as advertisements that the business wishes to place with the content provider without requiring the business to disclose customer data in an unencrypted form, and any non-matched data can remain confidential.

[0005] One embodiment of the invention is system for anonymously sharing user profile data among a plurality of entities. The system comprises a plurality of data appliances located at a plurality of entities with user profile data and a server configured to communicate with each of the plurality of data appliances to facilitate sharing of user profile data among the plurality of data appliances. The plurality of data appliances further includes a first data appliance that is configured to: receive, from a first entity, first user profile data for a first group of users associated with the first entity, the first user profile data including names and

addresses of the first group of users; encrypt the first user profile data for each of the first group of users into a first encrypted identifier; and send the first encrypted identifiers to the server. The plurality of data appliances also includes a second data appliance that is configured to: receive, from a second entity, second user profile data for a second group of users associated with the second entity, the second user profile data including names and addresses of the second group of users; encrypt the second user profile data for each of the second group of users into a second encrypted identifier with the same encryption used by the first data appliance, so that common user profile data between the first and second user profile data are converted into identical encrypted identifiers; receive from the server the first encrypted identifiers; and locate identical identifiers from among the first and second encrypted identifiers to generate an anonymous list of common users between the first and second groups of users, whereby the list can be used to customize content provided by the second entity to the users associated with the first entity.

[0006] Another embodiment is a system for anonymously sharing user profile data among a plurality of entities. The system comprises a plurality of data appliances and a server configured to receive data from and transmit data to the plurality of data appliances. The plurality of data appliances comprises a first data appliance that is configured to: receive, from a first entity, first personal identifiable information related to a first group of persons; transform the first personally identifiable information into first encrypted data via an encryption process, the first encrypted data comprising an identifier for each of the first group of persons; and send the encrypted data to the server. The plurality of data appliances also comprises a second data appliance that is configured to: receive, from a second entity, second personally identifiable information related to a second group of persons; transform the second personally identifiable information into second encrypted data with the encryption process used by the first data appliance, the second encrypted data comprising an identifier for each of the second group of persons; receive from the server the first encrypted data; and use the first and second encrypted data to anonymously generate list data related to common persons between the first and second groups of persons, so that the list data can be

used to customize information provided by the second entity at a direction of the first entity.

[0007] Yet another embodiment is a method for sharing anonymized user profile data. The method comprises: receiving at a first data appliance, first personally identifiable information related to a first group of persons; transforming the first personally identifiable information into first encrypted data via an encryption process, the first encrypted data comprising an identifier for each of the first group of persons; transmitting the first encrypted data from the first encrypted data to a second data appliance; receiving, at the second data appliance, second personally identifiable information related to a second group of persons; transforming the second personally identifiable information into second encrypted data with the encryption process, the second encrypted data comprising an identifier for each of the second group of persons; and using the first and second encrypted data to anonymously generate list data related to common persons between the first and second groups of persons, so that the list data can be used to customize information provided by the second entity at a direction of the first entity.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] Specific embodiments of the invention will now be described with reference to the following drawings, which are intended to illustrate embodiments of the invention, but not limit the invention:

[0009] Figure 1 is a flow diagram illustrating one embodiment of the marketing data sharing architecture;

[0010] Figure 2 is a flow diagram illustrating the process of loading and matching data with the user ID pass-through feature according to one embodiment;

[0011] Figure 3 is a flow diagram illustrating one embodiment of a hybrid real time targeting model;

[0012] Figure 4 is a flow diagram illustrating one embodiment for data sharing with a data partner;

[0013] Figure 5 is a flow diagram illustrating another embodiment for data sharing with a data partner;

[0014] Figure 6 shows an example audience select tool in accordance with one embodiment; and

[0015] Figure 7 is a flow diagram illustrating the use of data sharing to generate customized email marketing in accordance with one embodiment.

[0016] Figures 8A and 8B show examples of audience reports output by the system in accordance with one embodiment.

[0017] Figure 9 is block diagram of an example computing system of an embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0018] Embodiments of the invention will now be described with reference to the accompanying figures, wherein like numerals refer to like elements throughout. The terminology used in the description presented herein is not intended to be interpreted in any limited or restrictive manner, simply because it is being utilized in conjunction with a detailed description of certain specific embodiments of the invention. Furthermore, embodiments of the invention may include several novel features, no single one of which is solely responsible for its desirable attributes or which is essential to practicing the inventions herein described.

System Overview

[0019] The effectiveness of online advertising has been shown to improve significantly when an advertisement ("ad") is customized for a consumer based on known data about that consumer. Ad customization can be performed by either the sellers or buyers of online advertising. Sellers of online advertising include (but may not be limited to) web publishers, portals and ad networks. Buyers of online advertising are advertisers and their agencies. The amount of information that parties have about the consumers they interact with differs based on the type of business they are. An advertiser may have an established database of its customers, both online and offline, that collects information about the consumer's interaction with that advertiser's business. Additionally, an online publisher that

requires its users to login to its website as members may have detailed information on each user member. By contrast, an ad network may not have a simple way of collecting customer data other than via observed behaviors.

[0020] Regardless of the relative volume of known consumer profile data, for reasons of existing privacy policies and/or for competitive and strategic considerations, companies are traditionally reluctant to share consumer data without the existence of some trusted third party that can protect the confidential information of each contributor. For example, an advertiser A may share a number of common customers with a publisher B. Advertiser A may wish to only target its ads to those common customers on publisher B's website. One way of to achieve this is for A to send B a complete list of its customers and have B match the list against its own member list. However, Advertiser A may be reluctant to share such data with Publisher B for privacy, competitive and strategic reasons. However, if C, a trusted third party, took responsibility for merging the consumer data from Advertiser A and from Publisher B, identifying the overlap, and providing the customization data back to Publisher B in a manner through which consumer identifying information is anonymized, then the parties may be more inclined to use their known data for ad customization. In this manner, A will ensure that B will only know the common users/customers without seeing all of A's customers. If this capability could be made available across a large number of ad sellers, then an advertiser could make highly targeted ad buys across multiple ad sellers.

[0021] Embodiments of the invention facilitate confidential and secure sharing of de-personalized and/or anonymous customer profile data between companies for the purposes of improving ad targeting. Companies that would share such data could include buyers of media (e.g., advertiser), sellers of media (e.g., publisher, portal, or ad network), multiple advertisers (in a co-operative type model), or multiple sellers of media. Embodiments of the invention enable an entity to de¬personalize and/or anonymize its own consumer data and match that data to a third party's consumer data via anonymous keys. As such, the user profile data can be shared to improve ad customization without the need to disclose sensitive data in an unencrypted form.

[0022] Embodiments of the invention comprise a network of marketing data appliances (MDAs) that connect to each other to provide data matches among various entities. The MDAs perform data standardization and encryption to de¬ personalize the data. An MDA can also use an anonymous key, common to all MDAs to match similar data among MDAs. An entity that wishes to participate in the sharing of data can install the MDA within its secured network environment or can use a central installation. Alternatively, an entity may also share data using MDAs that are hosted off-site via secured transmission channels. The MDAs may be interconnected to one another, as well as to one or more marketing bureaus that serve as hubs that support the anonymization and matching processes performed at the local MDAs. In one or more embodiments, marketing bureaus are data processing entities with computing capacity (computer servers) that can handle matching and anonymization functions. Additional details relating to marketing bureaus will be provided later in the specification.

[0023] Embodiments of the data sharing system are beneficial in several ways. First, they enable media buyers to target against their own criteria instead of or complementary to the media's available criteria, thereby reducing media waste and increasing the precision and response of their advertising. Second, they enable media buyers to focus their media purchases without the need to disclose confidential user profile data about their customers. Third, the various embodiments create a virtual network that links disparate entities with potentially different data formats and provides a standardized way to exchange ad targeting and/or other relevant data. Finally, the various embodiments create a dynamic data accounting method that enables both media buyers and sellers to instantly view the number of targeted users at various publisher or portal sites through the use of an audience selector tool.

[0024] Although this disclosure provides example embodiments for Internet or online advertising, embodiments of the invention are not so limited to those environments. For example, embodiments of the invention can be implemented in any environment with addressable devices. For example, embodiments may be used to target advertisements served to wireless devices such

as cell phones and PDAs, cable television and satellite TV set top boxes, gaming consoles, and other portable devices such as music players and electronic book readers. Embodiments of the invention may be used in numerous environments, even those without "addressable" systems or those in "non-digital" media. Embodiments can be used in non-digital environments such that anonymized marketing data can be used to conduct, for example, phone or postal mail advertising campaigns. This is because, in addition to real-time request/response handling for ad and/or content customization, some embodiments provide productionized and efficient merge, purge, and data enhancement capabilities that can function in "batch" mode of operations, which can be performed daily/nightly/weekly or incrementally (every n hours).

System Architecture and Process

[0025] Figure 1 depicts the components of the data sharing architecture. Although a marketing bureau 102 is shown as connecting an advertiser 104 to a portal or publisher 106, in Figure 1, the marketing bureau 102 can connect other entities shown in the figure as well. The advertiser 104 and the portal or publisher 106 are highlighted in Figure 1 as examples. As shown, the advertiser 104 has a member database 114 and the portal or publisher 106 has its own member database 116 as well.

Anonymization of User Profile Data Provided by Advertisers

[0026] In one embodiment, to enable anonymized data sharing through the marketing bureau 102, the advertiser 104 installs a MDA 108 within its own environment, which may be protected by a network firewall. The bureau 102 may host a computer server that acts as a central repository for all information about each participating entity's address market. The information may include market segment data, for example. As described below, the data sharing architecture includes a network of interconnected MDAs that enable all connected entities to share data. The anonymized sharing and data matching process proceeds as

follows. In step 1, the advertiser 104 may upload, from its member database 114, any (1) personally identifiable information (PII) data such as member names, postal addresses, and (2) additional data such as segments onto the MDA 108. The uploaded data will be referred to as marketing data in this disclosure, and marketing data may include other non-PII data such as IP addresses, email addresses, cookie IDs, etc. In other embodiments, the PII may include email addresses, user IDs, social security numbers, IP addresses, phone numbers, etc. As used herein, "profile data," "customer data," and "consumer data" are used to refer generally to both PII and marketing data.

[0027] In step 2, as these records are being uploaded, the MDA 108 may derive bureau IDs (BIDs) by encrypting, through for example a forward encrypting hash algorithm such as SHA, some or all of the member's PII, e.g., name and postal address information. In another embodiment, a proprietary hash algorithm is used. For example, a name "John Doe" and an address "123 Main St." may be hashed into a resultant BID string "A348BEF6" so that the name and address cannot be deciphered from reading the resultant string. Once the BIDs are derived, the encryption process then purges the uploaded names, postal addresses, and other PII data. Because in various embodiments the encryption hashing algorithm is not data dependent, matching may be performed on other member/customer profile data such as membership IDs, vehicle IDs, cookie IDs, phone numbers, and/or email addresses. Any of the identifiable information that is used as input for the match, like a cookie ID or an email address, is subsequently converted into a BID. In one embodiment, if only name and ZIP code are provided, the MDA 108 first attempts to locate the complete postal address using the name and ZIP code and then performs the hashing process.

[0028] In one embodiment, the encryption process of step 2 takes place while the uploaded marketing data records are still in volatile memory such as in the MDA's random access memory (RAM). As such, sensitive records containing PII such as names and addresses are not placed in long term storage of the MDA. In one embodiment, the MDA does not need to use the full set of marketing segment data from the marketing bureau server in the encryption process.

[0029] After the encryption processing has completed, the MDA 108 stores records that include BIDs and the advertiser appended custom segment data and/or generic segment data appended by the MDA. For example, if the advertiser 104 were a credit reporting agency, it might append custom segment data that indicates whether a consumer is a free trial, paid, or cancelled member of its credit reporting subscription service. Also, the MDA 108 may append generic marketing data (segments) from other sources. The appended marketing segment data may be selected by the advertiser. For example, while an advertiser may not have its own custom segment data, it may instruct the MDA to append segment data identifying "New Parents" or "New Homeowners." The MDA 108 may use a localized copy of marketing segment data that is periodically updated by a remote server. The localized copy may be encrypted.

[0030] If any of the advertiser's appended data is deemed sensitive, the MDA 108 may apply additional security hashing to the appended data to provide a further tier of protection. The MDA may be configured so that no personally identifiable information (PII) is passed outside of the advertiser's environment.

[0031] In step 3, in one embodiment, the now anonymized advertiser's segment data is then propagated, through the marketing bureau 102, to some or all of participating entities that are connected to the data sharing network, including the publisher, portal, or ad network from which the example advertiser may wish to buy media. In one embodiment, steps 1-3 as described above may be performed as part of a nightly batch processing job. However, one or more the steps may be performed in real time or as part of a batch job executed at different intervals (e.g. weekly). Once the initial matching and propagation steps are accomplished upon an entity joining the data sharing network, subsequent matching and propagation may be performed on a smaller subset profile data within the member database that includes recent changes.

[0032] Embodiments of the invention also allow advertisers to identify some or all of its uploaded marketing data as the ideal or targeted modeling criteria for expanded or "look-alike" matching. For example, an advertiser may specify that ZIP codes be used as an expanded matching criterion, so that the matching process

performed by the MDA located at the publisher, portal and/or ad network as further described below returns matching results with additional persons who may live in or near the ZIP code areas of those consumers identified within the advertiser's data. Similarly, an advertiser may select one or more segments on which an expanded matching may be performed (e.g. matching on a "New Parents" or "New Homeowners" segment). In one embodiment, the look-alike matching uses demographic and consumer attributes (e.g. age, gender, income, purchase preferences, etc.) to identify additional persons who are similar to those in the matched results.

[0033] In one embodiment or more embodiments, an advertiser can identify ideal or targeted criteria through one of two methods. First, an advertiser can identify ideal or targeted criteria by inserting data flags into the uploaded marketing data records as part of the upload process described above. The uploaded data records may be termed a "primary list" in one or more embodiments. Second, an advertiser can provide a secondary list in conjunction with the primary list, with the secondary list providing a list of records on the primary list that have the ideal or targeted criteria.

Anonymization of User Profile Data Provided by Publishers and Portals

[0034] In one embodiment, similar to the advertisers, publishers and portals also install MDAs locally and possibly within their firewalls. In one embodiment, similar to steps 1-3, the portal or publisher 106 undertakes step 4 to upload its subscriber or member file onto an MDA 110 and in step 5 a similar encryption process takes place within MDA 110. The subscriber or member file may include marketing data, which may include PII data and other additional data such as segment data. In one embodiment, a forward encrypting hash algorithm (e.g., SHA) is applied to some or all of the subscriber's or member's PII, e.g., name and postal address information, to derive BIDs. Using the example from above, a "Joe Doe" at "123 Main St." may be hashed into a resultant BID string "A348BEF6," which, as described below, is used to match the BID previously generated at the advertiser's MDA. In other embodiments, the PII may include email addresses, user

IDs, social security numbers, IP addresses, phone numbers, etc. In one embodiment, if only name and ZIP code are provided, the MDA 110 first attempts to locate the complete postal address using the name and ZIP code and then performs the hashing process. In one embodiment, the derived BIDs replace the names and postal addresses in RAM, ensuring that no names, postal addresses or other PII are stored in non-volatile memory storage. The MDA 110 may include a localized copy of marketing segment data that is periodically updated by a remote server. The localized copy may be encrypted.

Joining / Matching User Profile Data

[0035] In step 6, the BID is then used as the connecting key between the disparate data sets from the advertiser 104's member and segment data and those of the portal or publisher 106. In particular, the MDA 110 of the portal or publisher 106 uses the BIDs to join or match the incoming data (from the advertiser 104) with those from the member database 116 of the portal or publisher 106. Although not shown in Figure 1, the same BID match process can be used to match data between an advertiser and an ad network as well. In one embodiment, once the matching ends, the BIDs are purged, leaving the publisher, portal or ad network's own identifier for a particular consumer and the advertiser's client segment for that same consumer. Thus, the matching is done such a way any non-matched data of the advertiser remains confidential and not revealed to the publisher or portal.

[0036] After the processing has completed, the MDA 116 contains records that include BIDs and user IDs from the publisher or portal 106 and ad segment. This creates a set of valid BID to user ID mappings for the network. In one embodiment, the BIDs are then purged, leaving only the publisher, portal or ad network's own identifier for a particular consumer (e.g., user ID) and the advertiser's segment for that same consumer. In step 7, the portal or publisher 106 may then export the list of joined user IDs and the corresponding advertiser's segment data to its proprietary ad server 120 or to an outsourced ad sever. Alternatively, as shown

later in Figure 3, the joined user IDs and the corresponding advertiser's segment data may be retrieved in real time through the use of a compute cluster.

[0037] With the data matching completed, advertisers can then include or exclude their own member households or otherwise target their own data in their media buys with publishers or portals. The process may proceed as follows. The advertiser 104 may place a media buy insertion order with the portal or publisher 106. The portal or publisher 106 may possibly stipulate to not target existing members of the advertiser 104. The portal or publisher 106 may then export a list from its local MDA 110, comprised of only its own members that are also known members of the advertiser 104, and upload the list onto its ad server as an "exclusion target" for a campaign, where segment(s) of customers/members are excluded from a media campaign (e.g. existing customers/members are excluded).

[0038] The MDAs make up a distributed network that facilitates businesses' ability to connect with each other's data in real time or batch mode and in a secure manner that de-personalizes consumer information throughout the processing steps. While Figure 1 depicts a data flow from an advertiser to a portal/publisher, embodiments of the invention can facilitate data sharing between any entity depicted, e.g., between two advertisers, between two ad networks, or between two publishers/portals.

[0039] In one embodiment, MDA ensures that any set of data elements does not constitute a signature. This means that, for example, any set of data elements must be the same for at least 100 users or 0.05% of the users, whichever is greater. In one embodiment, if a data element set has less than 100 users, that element is not created so as to protect the privacy of the few users that may constitute that element.

[0040] In one embodiment, the matching process takes into account the generic or custom segment data and/or expanded matching criteria. Thus for example, before or after identifying the overlap in users/members/subscribers between the advertiser and the publisher/portal, the matching process may apply criteria to narrow or expand the match results. The matching process may narrow by filtering the results through segment matching. For example, the results may be

narrowed down to include those records with matching segments only. As discussed above, the segments may be custom (created by the advertisers) or generic (selected by the advertisers from a list of available segments). The matching process may also expand the overlap results by using expanded or "look-alike" matching as previously described. In these embodiments, the matching process adds to the overlap list users/members/subscribers of the publisher or portal that do not already appear on the overlap list but nonetheless match one or more ideal or targeted criteria as specified by the advertiser. In one or more embodiments, the system is highly customizable and the advertiser can select a combination of narrowing or expanding matching processes as described above.

Ad Network

[0041] Although ad networks sell media to advertisers across publisher websites with their networks and have large ad distribution capability, they generally have very limited or no PII such as names or postal addresses for their "members," which in this case include households or users that are tracked by the ad networks. Instead, for each end user, ad networks generally create a unique user ID that they store locally and in cookies on the end user's computer. Cookies are small text files that are deposited onto consumers' computers and generally contain basic identifying information such as user IDs, time stamps, etc.

[0042] One embodiment directed at the ad network model takes into account information that the ad networks may pass back to advertisers. In addition to the process described above in conjunction with Figure 1, this embodiment allows for the ad network to pass its user ID to back to the advertiser when an end user clicks on the advertiser's ad.

[0043] Figure 2 illustrates this additional user ID pass-through feature. User ID matching steps 1-6 are substantially similar to the corresponding steps illustrated in Figure 1. After they are completed, the advertiser 104 may arrange for the ad network 124 to pass its user ID to the advertiser 104 in the "E" series of steps shown in Figure 2. The user ID may be passed via a cookie or other suitable means. In step E1, the advertiser 104 places an insertion order for a media buy with

the ad network 124. In step E2, the ad network exports a list of user IDs with the advertiser's segments to a publisher-partner site 124. In step E3, when a visitor clicks on an ad served by on the publisher-partner site 124, the visitor is re-directed to the advertiser's site 126. During the re-direction, the advertiser 104 receives the ad network's user ID for that visitor. In step E4, the user ID is carried through to the visitor's session with the advertiser, which may end with a registration or lead form 130 for service sign up. Assuming the visitor completes the registration or lead form 130, the advertiser 104 receives his or her marketing data including PII, e.g., name and postal address, and in step E5 passes the newly received marketing data to its local MDA 108.

[0044] In one embodiment, in the MDA 108 the above described anonymization process would be executed the newly received marketing data. In one embodiment, after the anonymization processing is executed in the MDA's RAM, the MDA may contain a BID, the advertiser's segments, and the ad network's user ID. In step E6, this newly processed information is passed through the marketing bureau to the ad network 124, so that it can be joined, in the ad network's local MDA, with a forward hashed version of the ad network's user ID. After the new data match in step E6, the ad network would have the ability to connect its user IDs with the advertiser's segments.

[0045] The "F" series of steps illustrate an alternate embodiment in which the advertiser is using the data sharing system to target specific segments on the publisher-partner site 126 using data obtained in the "E" series of steps. In step F1, the advertiser 104 may place a media buy with the ad network 124, targeting its members with, for example, upsell offers. In step F2, the ad network 124 may export a list of its IDs and the advertiser's members that are the targets for upselling, and upload the list to the ad server for the publisher-partner site 126. When users who are members of the advertiser 104 visit the publisher-partner site 126, they may see ads that are targeted to them for upselling, leading them to the advertiser's site 128.

Data Transmission

[0046] In one embodiment, data that are transmitted from the advertiser to the publisher or portal are fully encrypted. These data may be passed using an encryption scheme such as GPG (GnuPG) and the keys to decrypt the data exist on the target MDAs. For example, in Figure 1, the decryption keys reside on MDA 110. Servers that receive the data in transit do not have the keys required to decrypt the data and act as a pass-throughs to minimize the amount of firewall rules required to accommodate MDAs that receive the data.

Hybrid Real Time Targeting Model

[0047] In one embodiment, a publisher, portal, or an ad network may have a compute cluster 138 installed within its environment in addition to a MDA. An example embodiment with a compute cluster 138 is illustrated in Figure 3. BID matching steps 1-6 shown in Figure 3 are substantially the same as the corresponding numbered steps depicted in Figure 1. However, instead of a simple export to the ad server in step 7, a different process is performed on a per-transaction basis as illustrated in the following "G" series of steps depicted in Figure 3.

[0048] In step G1, the advertiser 104 may place a media buy with the portal or publisher 106. In step G2, when a user visits the portal or publisher site 106, the portal or publisher 106 may send a request to the compute cluster 138 with the user ID that the publisher 106 has assigned to the user, along with the user's IP address. If the compute cluster 138 fails to find a match on the user ID, it may send the IP address to the marketing bureau and retrieve household level targeting or inferred geo-demographic targeting of consumer data. The process of obtaining inferred geo-demographic targeting is further described in co-pending U.S. Patent Application entitled "SYSTEMS AND METHODS FOR REAL TIME SEGMENTATION OF CONSUMERS," No. 12/118,585, filed May 9, 2008, the disclosures of which are hereby fully incorporated by reference. Once the

appropriate targeting data is returned to the ad server 120, an ad may be selected based on the targeting data and served in step G3.

[0049] With the compute cluster, any publisher, portal, or ad network can offer three tiers of insights to its advertisers, namely by custom segment (Figure 1), by household level targeting data (e.g., through segment data made available by the compute cluster), and by inferred geo-demographic targeting data (e.g., through functions provided by the compute cluster) (Figure 3). Having a compute cluster also allows the publisher, portal, or ad network to retrieve advertiser targeting on a transaction-by-transaction basis, rather than exporting a file from its MDA to its ad server.

Localized Copy of Marketing Segment Database

[0050] As mentioned above, in some embodiments, each MDA can include a local encrypted copy of a marketing segment database. Thus, in addition to submitting marketing data including PII such as names and addresses from their membership databases, advertisers could then also retrieve the cleansed records (e.g., hygiene - cleanse invalid records, standardization - standardize data elements such as address suffix, and verification - verify the data elements with an external source) along with data enhancement and even custom scores in real time, within their own local environments. For example, the MDA may contain a local copy of segment market data that may be returned as part of the data anonymization process. Similarly, the MDA may perform a process of standardizing the input addresses and may return addresses that conform to U.S. Postal standards, for example. In some embodiments, custom scores may also be returned as part of the process. The functions and features of an individual compute cluster are customizable and may be dynamically updated through data sent from the marketing bureau 102.

Data Partners

[0051] Figure 4 illustrates another embodiment where a data partner 142 is involved in the process. In this embodiment, an advertiser 162 places ads on a

publisher 152 while using the data partner 142's segment data to target the ads. The BID matching steps 1-6 shown in Figure 4 are substantially the same as the corresponding numbered steps depicted in Figure 1, except in Figure 4 the matching is conducted between members of the data partner 142 and the publisher 152.

[0052] Once the matching steps are accomplished, the process proceeds as illustrated in the "H" series of steps in one embodiment. In step H1, the advertiser 162 places a media buy insertion order with the publisher 152, instructing it to target the data partner 142's members. In step H2, the publisher 152 exports a list from its local MDA 154, comprised of only user IDs from the publisher's member database 156 that are known members of data partner 142, and uploads the list onto its ad server 160 as the target for a campaign for the advertiser 162 on its site. In step H3, acquisition marketing traffic from the display of those targeted ads is driven to the advertiser 162.

[0053] Figure 5 illustrates another example embodiment that connects an advertiser and a data partner 172 to an ad network 182. In this embodiment, an advertiser and data partner 172 places ads on an ad network 182. The BID matching steps 1-6 shown in Figure 5 are substantially the same as the corresponding numbered steps depicted in Figure 1. Note that the ad network 182 is able to accomplish the matching steps for the advertiser and data partner 172 because it has access to member data. Some ad networks may not have PII data such as name and address data on which they can conduct the initial BID matching.

[0054] Once the matching steps are accomplished, the process proceeds as illustrated in the "I" series of steps in one embodiment. In step I1, the advertiser 172 places a media buy insertion order with the ad network 182, instructing it to target a specific segment of the advertiser and data partner 172's members. In step I3, the ad network 182 exports a list from its local MDA 184, comprised of user IDs from the advertiser and data partner's member database 176, and uploads the list onto its ad server 190. In step I3, acquisition marketing traffic from the display of those targeted ads are driven to the advertiser and data partner 172.

Customized Emails

[0055] Figure 6 illustrates another embodiment in which the data sharing system is applied to provide targeted advertising through customized emails. In this embodiment, a customized email provider 192 purchases ads from an portal / publisher 196 that will be placed into the email provider 192's own emails instead of web pages. The segments used in this matching process are provided by an advertiser A1 194 that wishes to use the email provider 192 to send custom emails on A1's behalf. The BID matching steps 1-6 shown in Figure 7 are substantially the same as the corresponding numbered steps depicted in Figure 1. In step 7, matched data from the portal / publisher 196 are exported to a server that sends customized ads to emails generated by the email provider 192.

Audience Selector Tool

[0056] With a network of MDAs installed in various advertisers, ad networks, publishers and online portals and interconnected through the marketing bureau, sharing of user profile data may be greatly enhanced and online media buys may be made more efficient. In addition, advertisers may be able to query, through an audience selector tool, the data sharing system to determine how many unique users exist within the desired target entities. For example, an ad buyer may be able to see how many unique users exist on various portal and/or publisher sites that are also free trial members of its services. An example audience selector tool is shown in Figure 7.

Feedback Data - Match Data and Conversion Metrics

[0057] In addition to the audience selector tool, which can assist in pre-purchase planning and allocating decisions, embodiments also provide feedback data to assist advertisers and other participants to monitoring match rates and return on investment. In one or more embodiments, an advertiser can receive feedback on the marketing data uploaded. The feedback data provided by embodiments of the MDA include the number of persons within the uploaded data who match certain segments. Figure 8A provides an example of the type of match data provided. As

shown, an example advertiser is receiving a report on the number of matches with a publisher and the detailed breakdown of matches by segments.

[0058] In one or more embodiments, the feedback data provided is based on conversion metrics. To receive conversion metrics data, an advertiser can identify a number of persons who have recently engaged in conversion activities. For example, an advertiser can identify persons who have recently signed up for paid services or filled out a form to request additional information as a result of its advertising efforts initiated through the system. An advertiser may identify such persons through, for example, the two mechanisms described in conjunction with Figure 1: (1) upload a secondary list of such persons or (2) identify such persons in the primary list by, for example, inserting flags into the data records. The MDA in one or more embodiments processes the uploaded information by cross-referencing it against the primary list(s) uploaded from previous time period(s) and returning an estimated percentage of conversion to the advertiser.

[0059] For example, a MDA may receive from an advertiser a list of persons who have engaged in conversion activities in the last week. The DNA may cross reference the new conversion list against the primary list from last week's campaign and return one or more example conversion metrics as shown in Figure 8B. As shown in the figure, the metrics calculated include a tally of those who visited the site, those who signed up for trial services and those who signed up for paid services. As shown, the metrics results may also include break-down by segments for individual conversion activities. The metrics on conversion activities are customizable and can be used to track any type of activities. For example, when used in contexts outside of internet advertising, a cable television operator may track movie downloads and a wireless service provider may track ringtone or song downloads. Metrics calculations can also be performed at various frequencies, for example, on a real-time or near real-time, daily, weekly, monthly, or yearly basis. The MDA in one embodiment aggregates the metrics over a period of time and provides advertisers a reporting tool for analyzing their return on investment in their advertising efforts.

[0060] As mentioned above, the various types of match and feedback data reports provided can be customized by advertisers and/or other interested parties. Similarly, portals, publishers and ad networks may be able to customize such reports and utilize them to provide potential advertisers characteristics of its membership. In addition, advertisers, portals, publishers and ad networks may use the match and feedback data to fine tune matching criteria in expanded ("look-alike") matching operations as described above.

System Architecture

[0061] Figure 9 is a block diagram illustrating a computer system 200 for implementing the marketing data appliances, bureau servers, ad servers, compute clusters, and other computer systems and devices illustrated in Figures 1 to 6 in accordance with one embodiment. The computer system 200 includes, for example, a personal computer that is IBM, Macintosh, or Linux/Unix compatible. In one embodiment, the computing system 200 comprises a server, a desktop computer, a laptop computer, a personal digital assistant, a kiosk, or a mobile device, for example. In one embodiment, the computing system 200 includes a central processing unit ("CPU") 202, which may include one or more conventional microprocessors. The computing system 200 further includes a memory 206, such as random access memory ("RAM") for temporary storage of information and a read only memory ("ROM") for permanent storage of information, and a mass storage device 210, such as a hard drive, diskette, or optical media storage device. Typically, the components and modules of the computing system 200 are connected to the computer using a standard based bus system 208. In different embodiments, the standard based bus system could be Peripheral Component Interconnect ("PCI"), MicroChannel, Small Computer System Interface ("SCSI"), Industrial Standard Architecture ("ISA") and Extended ISA ("EISA") architectures, for example. In addition, the functionality provided for in the components and modules of the computing system may be combined into fewer components and modules or further separated into additional components and modules.

[0062] The computing system 200 is generally controlled and coordinated by operating system software, such as Windows Server, Linux Server, Windows XP, Windows Vista, Unix, Linux, SunOS, Solaris, or other compatible server or desktop operating systems. In Macintosh systems, the operating system may be any available operating system, such as MAC OS X. In other embodiments, the computing system 200 may be controlled by a proprietary operating system. Conventional operating systems control and schedule computer processes for execution, perform memory management, provide file system, networking, I/O services, and provide a user interface, such as a graphical user interface ("GUI"), among other things.

[0063] The computing system 200 includes one or more commonly available input/output (I/O) devices and interfaces 216, such as a keyboard, mouse, touchpad, and printer. In one embodiment, the I/O devices and interfaces 216 include one or more display device, such as a monitor, that allows the visual presentation of data to a user. More particularly, a display device provides for the presentation of GUIs, application software data, and multimedia presentations, for example. The computing system 200 may also include one or more multimedia devices 204, such as speakers, video cards, graphics accelerators, and microphones, for example. In other embodiments, such as when the computing system 200 comprises a network server, for example, the computing system may not include any of the above-noted man-machine I/O devices.

[0064] In the embodiment of Figure 9, the I/O devices and interfaces 216 provide a communication interface to various external devices. In the embodiment of Figure 9, the computing system 200 is electronically coupled to the network 214, which may comprise one or more of a LAN, WAN, or the Internet, for example, via a wired, wireless, or combination of wired and wireless, communication link 212. The network 214 facilitates communications among various computing devices and/or other electronic devices via wired or wireless communication links.

[0065] According to Figures 1 to 6, requests are sent to the computing system 200 over the network 214. Similarly, results are returned over the network 214. In addition to the devices that are illustrated in Figure 9, the computing system

200 may communicate with other data sources or other computing devices. In addition, the data sources may include one or more internal and/or external data sources. In some embodiments, one or more of the databases, data repositories, or data sources may be implemented using a relational database, such as Sybase, Oracle, CodeBase and Microsoft® SQL Server as well as other types of databases such as, for example, a flat file database, an entity-relationship database, and object-oriented database, and/or a record-based database. For example, the above described data including at least the user profile data, the member data, the customer data, the personally identifiable information, and the encrypted data may be stored in various embodiments in these data sources.

[0066] In the embodiment of Figure 9, the computing system 200 also includes program codes and/or instructions stored on the mass storage device 210 that may be executed by the CPU 202. The program codes and/or instructions may include modules for performing user profile data anonymization, hashing, data encryption, data matching, and audience reporting as described above. These modules may include, by way of example, components, such as software components, object-oriented software components, class components and task components, processes, functions, attributes, procedures, subroutines, segments of program code, drivers, firmware, microcode, circuitry, data, databases, data structures, tables, arrays, and variables. Alternately, the modules may be implemented as separate devices, such as computer servers.

[0067] In general, the word "module," as used herein, refers to logic embodied in hardware or firmware, or to a collection of software instructions, possibly having entry and exit points, written in a programming language, such as, for example, Java, Lua, C or C++. A software module may be compiled and linked into an executable program, installed in a dynamic link library, or may be written in an interpreted programming language such as, for example, BASIC, Perl, or Python. It will be appreciated that software modules may be callable from other modules or from themselves, and/or may be invoked in response to detected events or interrupts. Software instructions may be embedded in firmware. It will be further appreciated that hardware modules may be comprised of connected logic units,

such as gates and flip-flops, and/or may be comprised of programmable units, such as programmable gate arrays or processors. The modules described herein are preferably implemented as software modules, but may be represented in hardware or firmware. Generally, the modules described herein refer to logical modules that may be combined with other modules or divided into sub-modules despite their physical organization or storage.

Conclusion

[0068] The foregoing description details certain embodiments of the invention. It will be appreciated, however, that no matter how detailed the foregoing appears in text, the invention can be practiced in many ways. As is also stated above, it should be noted that the use of particular terminology when describing certain features or aspects of the invention should not be taken to imply that the terminology is being re-defined herein to be restricted to including any specific characteristics of the features or aspects of the invention with which that terminology is associated. The scope of the invention should therefore be construed in accordance with the appended claims and any equivalents thereof.

WHAT IS CLAIMED IS:

1. A system for anonymously sharing user profile data among a plurality of entities, comprising:

a plurality of data appliances located at the plurality of entities with user profile data;

a server configured to communicate with each of the plurality of data appliances to facilitate sharing of user profile data among the plurality of data appliances, the plurality of data appliances comprising:

a first data appliance that is configured to:

receive, from a first entity, first user profile data for a first group of users associated with the first entity, the first user profile data including names and addresses of the first group of users;

encrypt the first user profile data for each of the first group of users into a first encrypted identifier; and

send the first encrypted identifiers to the server; and

a second data appliance that is configured to:

receive, from a second entity, second user profile data for a second group of users associated with the second entity, the second user profile data including names and addresses of the second group of users;

encrypt the second user profile data for each of the second group of users into a second encrypted identifier with the same encryption used by the first data appliance, so that common user profile data between the first and second user profile data are converted into identical encrypted identifiers;

receive from the server the first encrypted identifiers; and

locate identical identifiers from among the first and second encrypted identifiers to generate an anonymous list of common users between the first and second groups of users,

whereby the list can be used to customize content provided by the second entity to the users associated with the first entity.

2. The system of Claim 1 wherein the encryption is a cryptographic hash function.

3. A system for anonymously sharing user profile data among a plurality of entities, comprising:

a plurality of data appliances located at the plurality of entities;

a server configured to receive data from and transmit data to the plurality of data appliances, the plurality of data appliances comprising:

a first data appliance that is configured to:

receive, from a first entity, first personal identifiable information related to a first group of persons;

transform the first personally identifiable information into first encrypted data via an encryption process, the first encrypted data comprising an identifier for each of the first group of persons; and

send the encrypted data to the server; and

a second data appliance that is configured to:

receive, from a second entity, second personally identifiable information related to a second group of persons;

transform the second personally identifiable information into second encrypted data with the encryption process used by the first data appliance, the second encrypted data comprising an identifier for each of the second group of persons;

receive from the server the first encrypted data; and

use the first and second encrypted data to anonymously generate list data related to common persons between the first and second groups of persons, so that the list data can be used to customize information provided by the second entity at a direction of the first entity.

4. The system of Claim 3, wherein the second data appliance is further configured to generate the list data by matching the identifiers in the first encrypted data to the identifiers in the second encrypted data.

5. The system of Claim 3, wherein the first personally identifiable information comprise names and addresses related to the first group of persons.

6. The system of Claim 5, wherein the first data appliance is further configured to complete missing portions in the addresses in the first personally identifiable information before transforming the first personally identifiable information into the first encrypted data.

7. The system of Claim 3, wherein the first data appliance is further configured to delete the first personally identifiable information after transforming the first personally identifiable information into the first encrypted data.

8. The system of Claim 3, wherein the first data appliance is further configured to append segment data to the first encrypted data before sending the encrypted data to the server.

9. The system of Claim 8, wherein the second data appliance is further configured to:

receive, from the second entity, in addition to the second personally identifiable information, identifiers used by the second entity to identify the second groups of persons; and

use the list data to create a mapping of user identifiers received from the second entity to the segment data from the first entity.

10. The system of Claim 9, wherein the mapping is used to anonymously track responses to online advertisements and emails.

11. The system of Claim 8, wherein the second data appliance is further configured to identify additional persons referenced in the second encrypted data with personally identifiable information matching a criterion specified in the segment data, the additional persons not among the common persons in the list data.

12. The system of Claim 11, wherein the criterion is residing within an area with a common postal code.

13. The system of Claim 11, wherein the criterion is a type of consumer.

14. The system of Claim 11, wherein the criterion is an indication of consumer interest shown to a product.

15. The system of Claim 3, wherein the data appliance is configured to delete the first and second encrypted data after generating the list data related to common persons.

16. A method for sharing anonymized user profile data, the method comprising:

receiving at a first data appliance, first personally identifiable information related to a first group of persons;

transforming the first personally identifiable information into first encrypted data via an encryption process, the first encrypted data comprising an identifier for each of the first group of persons;

transmitting the first encrypted data from the first encrypted data to a second data appliance;

receiving, at the second data appliance, second personally identifiable information related to a second group of persons;

transforming the second personally identifiable information into second encrypted data with the encryption process, the second encrypted data comprising an identifier for each of the second group of persons; and

using the first and second encrypted data to anonymously generate list data related to common persons between the first and second groups of persons, so that the list data can be used to customize information provided by the second entity at a direction of the first entity.

17. The method of Claim 16, wherein the using further comprises generating the list data by matching the identifiers in the first encrypted data to the identifiers in the second encrypted data.

18. The method of Claim 16 wherein the first personally identifiable information comprise names and addresses related to the first group of persons.

19. The method of Claim 18, further comprising: completing missing portions in the addresses in the first personally identifiable information before transforming the first personally identifiable information into the first encrypted data.

20. The method of Claim 16, further comprising: deleting the first personally identifiable information after transforming the first personally identifiable information into the first encrypted data.

21. The method of Claim 16, further comprising: appending segment data to the first encrypted data before sending the encrypted data to the server.

22. The method of Claim 21, further comprising:

receiving, from the second entity, in addition to the second personally identifiable information, identifiers used by the second entity to identify the second groups of persons; and

using the list data to create a mapping of user identifiers received from the second entity to the segment data from the first entity.

23. The method of Claim 22, wherein the mapping is used to anonymously track responses to online advertisements and emails.

24. The method of Claim 21, wherein the second data appliance is further configured to identify additional persons referenced in the second encrypted data with personally identifiable information matching a criterion specified in the segment data, the additional persons not among the common persons in the list data.

25. The method of Claim 24, wherein the criterion is residing within an area with a common postal code.

26. The method of Claim 24, wherein the criterion is a type of consumer.

27. The method of Claim 24, wherein the criterion is an indication of consumer interest shown to a product.

28. The method of Claim 16, wherein the data appliance is configured to delete the first and second encrypted data after generating the list data related to common persons.

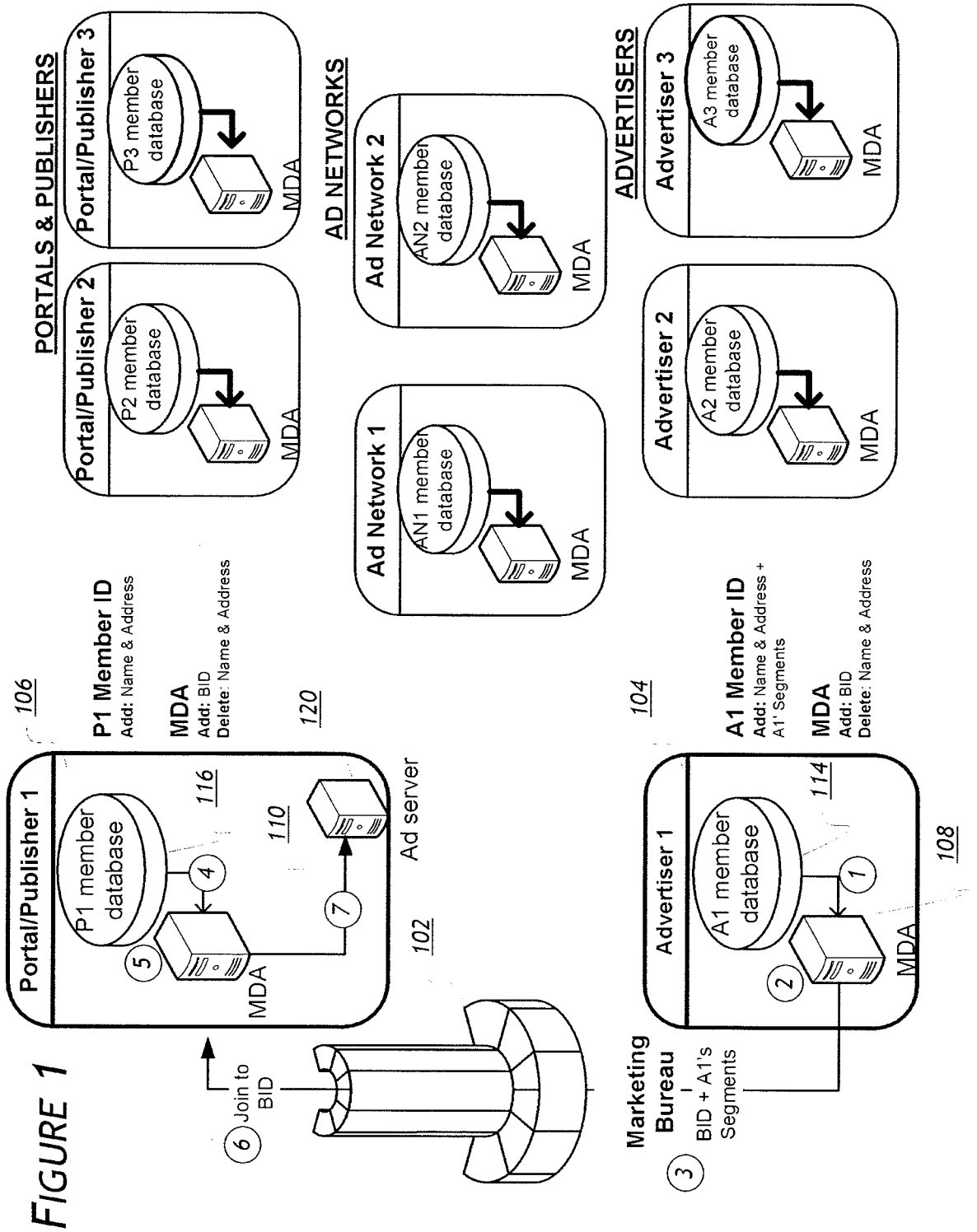

PORTALS & PUBLISHERS
Portal/Publisher 1
P1 member database
MDA
Portal/Publisher 2
P2 member database
MDA
Portal/Publisher 3
P3 member database
MDA
AD NETWORKS
Ad Network 1
AN1 member database
MDA
Ad Network 2
AN2 member database
MDA
ADVERTISERS
Advertiser 1
A1 member database
MDA
Advertiser 2
A2 member database
MDA
Advertiser 3
A3 member database
MDA
Ad server
Marketing Bureau
P1 Member ID
Add: Name & Address
MDA
Add: BID
Delete: Name & Address
A1 Member ID
Add: Name & Address + A1' Segments
MDA
Add: BID
Delete: Name & Address
Join to BID
BID + A1's Segments
102
104
106
108
110
114
116
120

FIGURE 1

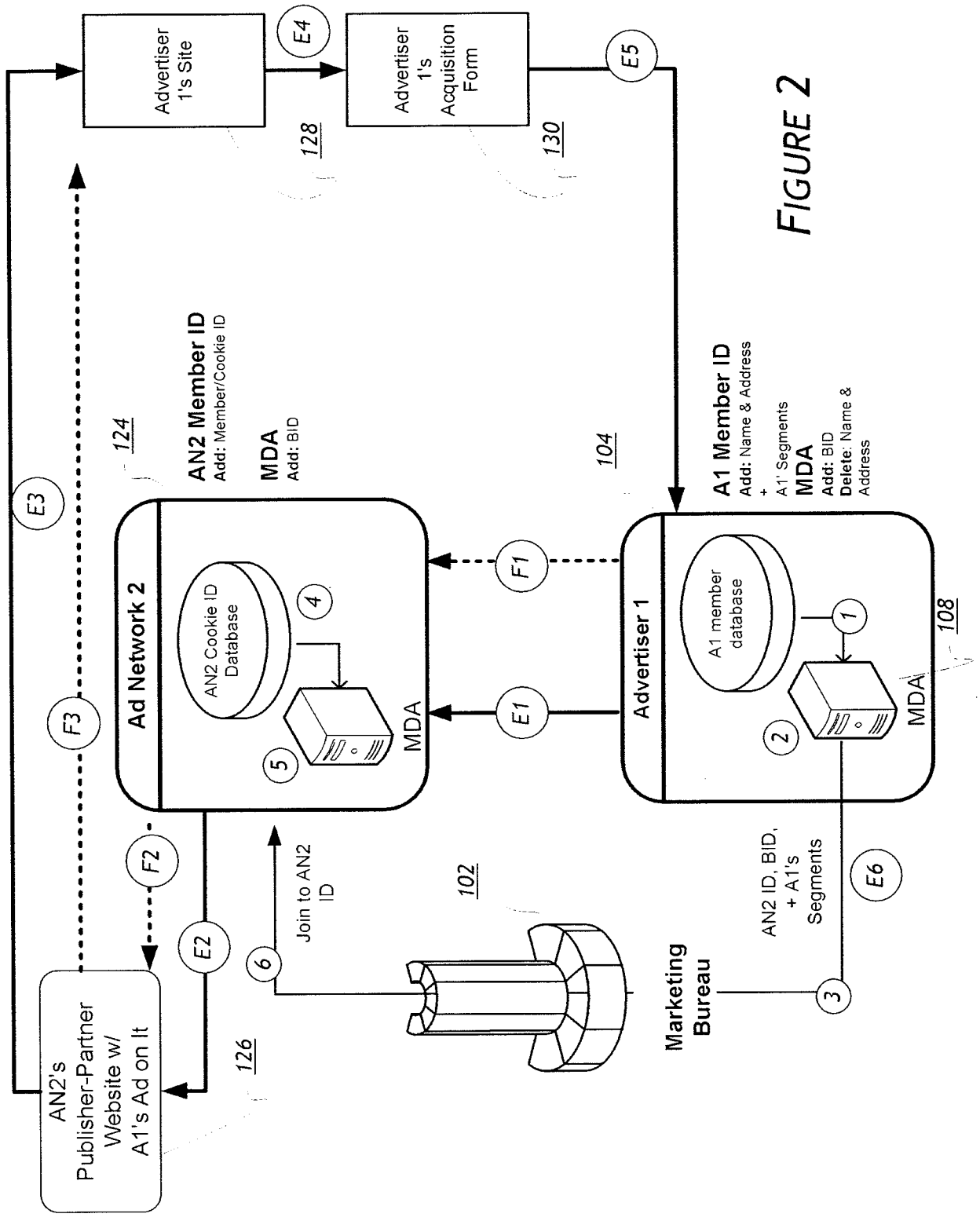

Advertiser 1's Site
E4
Advertiser 1's Acquisition Form
E5
128
130
E3
124
AN2 Member ID
Add: Member/Cookie ID
MDA
Add: BID
104
A1 Member ID
Add: Name & Address
+
A1' Segments
MDA
Add: BID
Delete: Name & Address
Ad Network 2
AN2 Cookie ID Database
4
5
MDA
F1
E1
Advertiser 1
A1 member database
1
2
MDA
108
F3
F2
E2
6
Join to AN2 ID
102
AN2 ID, BID, + A1's Segments
E6
3
AN2's Publisher-Partner Website w/ A1's Ad on It
126
Marketing Bureau

FIGURE 2

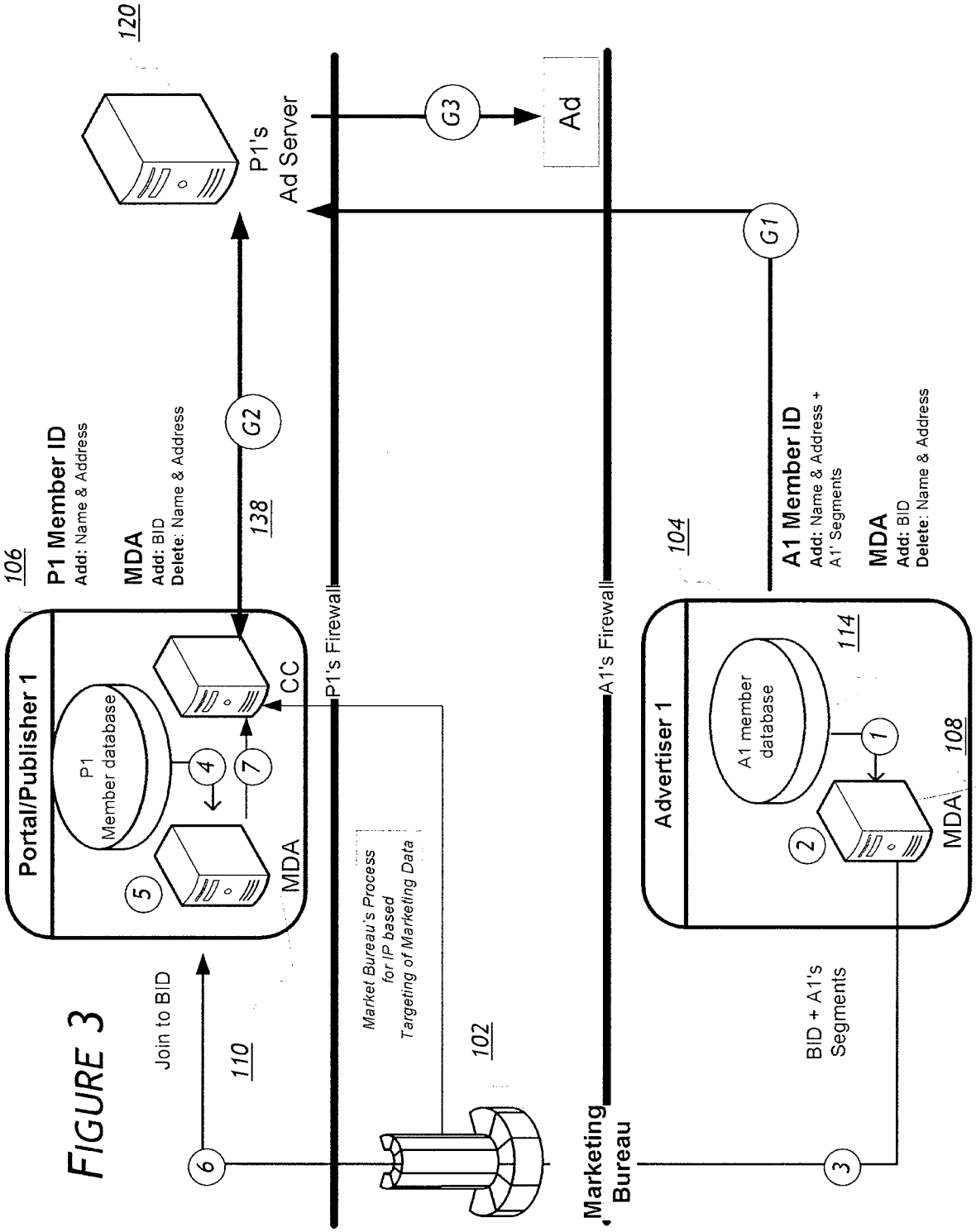

120
P1's Ad Server
G3
Ad
G1
G2
138
106
P1 Member ID
Add: Name & Address
MDA
Add: BID
Delete: Name & Address
Portal/Publisher 1
P1 Member database
CC
MDA
P1's Firewall
A1's Firewall
104
A1 Member ID
Add: Name & Address + A1' Segments
MDA
Add: BID
Delete: Name & Address
Advertiser 1
A1 member database
114
108
MDA
Join to BID
110
Market Bureau's Process for IP based Targeting of Marketing Data
102
BID + A1's Segments
Marketing Bureau

FIGURE 3

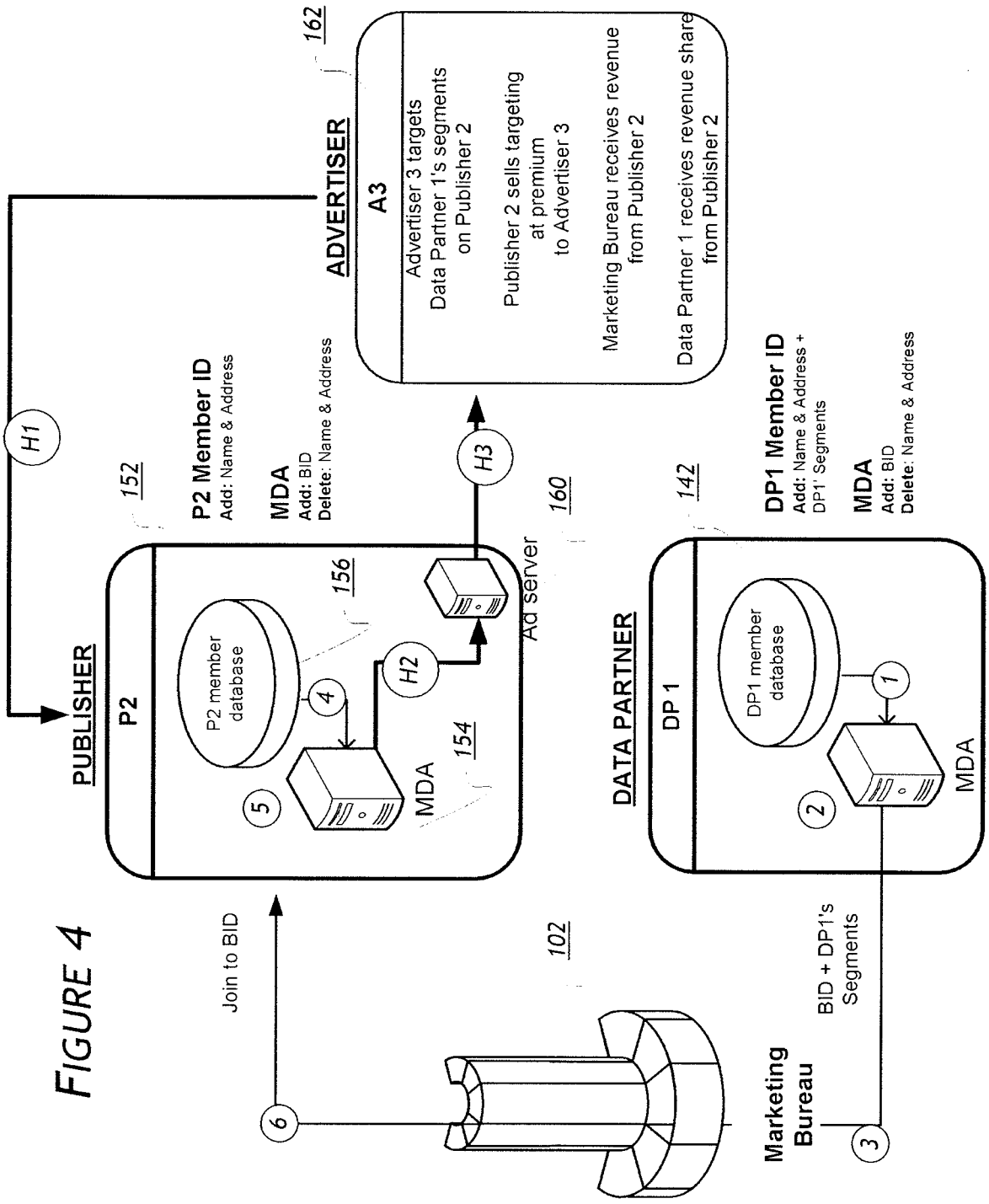

PUBLISHER
P2
152
P2 Member ID
Add: Name & Address
MDA
Add: BID
Delete: Name & Address
P2 member database
156
MDA
154
Ad server
160
ADVERTISER
162
A3
Advertiser 3 targets Data Partner 1's segments on Publisher 2
Publisher 2 sells targeting at premium to Advertiser 3
Marketing Bureau receives revenue from Publisher 2
Data Partner 1 receives revenue share from Publisher 2
DATA PARTNER
DP 1
142
DP1 Member ID
Add: Name & Address + DP1' Segments
MDA
Add: BID
Delete: Name & Address
DP1 member database
MDA
H1
H2
H3
1
2
3
4
5
6
Join to BID
BID + DP1's Segments
Marketing Bureau
102

FIGURE 4

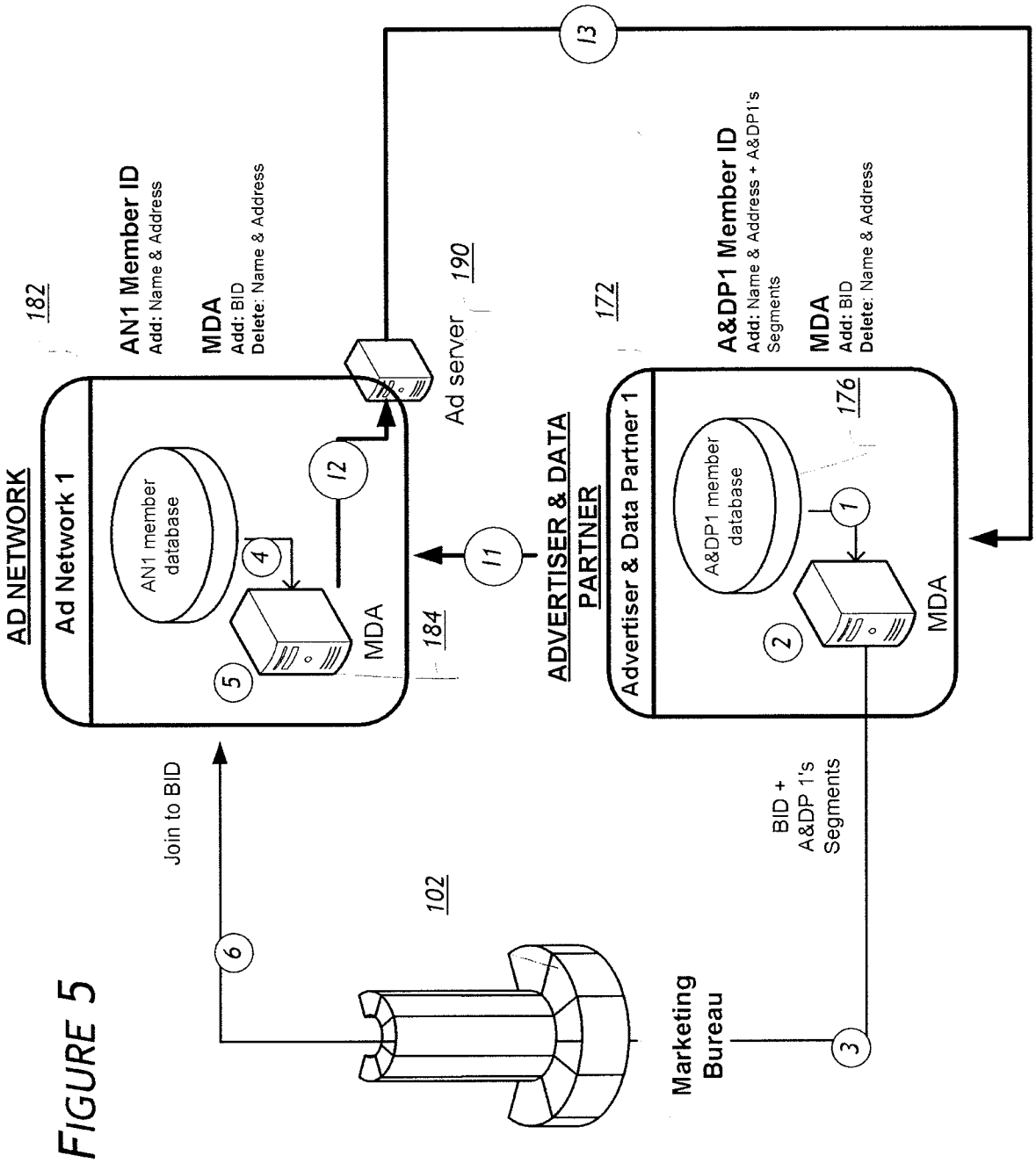

AD NETWORK
Ad Network 1
182
AN1 Member ID
Add: Name & Address
MDA
Add: BID
Delete: Name & Address
AN1 member database
MDA
184
Ad server
190
ADVERTISER & DATA PARTNER
Advertiser & Data Partner 1
172
A&DP1 Member ID
Add: Name & Address + A&DP1's Segments
MDA
Add: BID
Delete: Name & Address
A&DP1 member database
176
MDA
Join to BID
BID + A&DP 1's Segments
102
Marketing Bureau
1
2
3
4
5
6
11
12
13

FIGURE 5

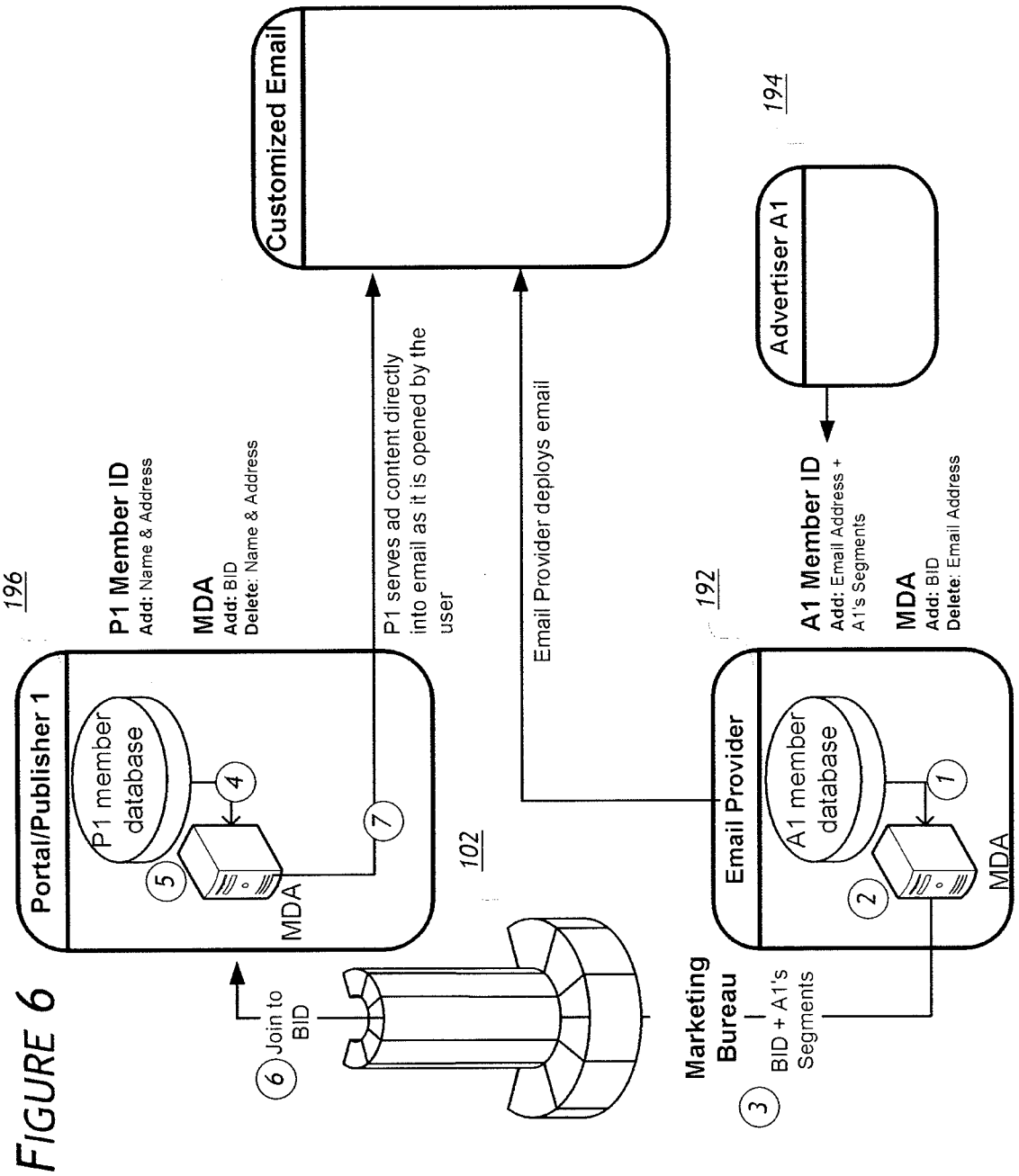

196
Portal/Publisher 1
P1 Member ID
Add: Name & Address
MDA
Add: BID
Delete: Name & Address
P1 member database
4
5
MDA
7
P1 serves ad content directly into email as it is opened by the user
Customized Email
194
Advertiser A1
Email Provider deploys email
192
Email Provider
A1 Member ID
Add: Email Address + A1's Segments
MDA
Add: BID
Delete: Email Address
A1 member database
1
2
MDA
102
6 Join to BID
Marketing Bureau
3 BID + A1's Segments

FIGURE 6

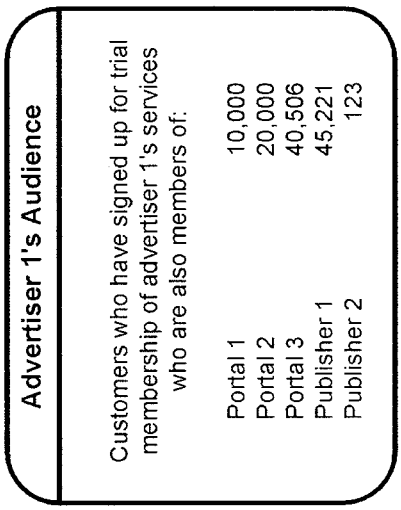

Advertiser 1's Audience
Customers who have signed up for trial membership of advertiser 1's services who are also members of:
Portal 1 10,000
Portal 2 20,000
Portal 3 40,506
Publisher 1 45,221
Publisher 2 123

FIGURE 7

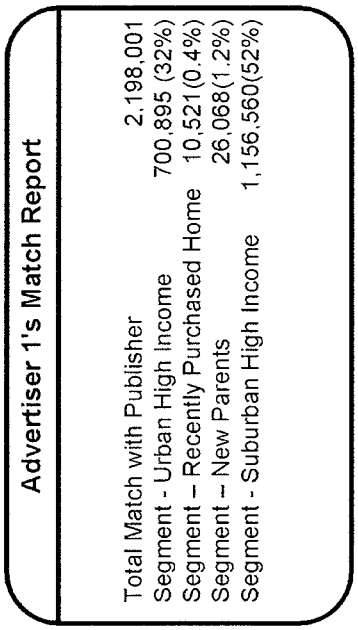


FIGURE 8A

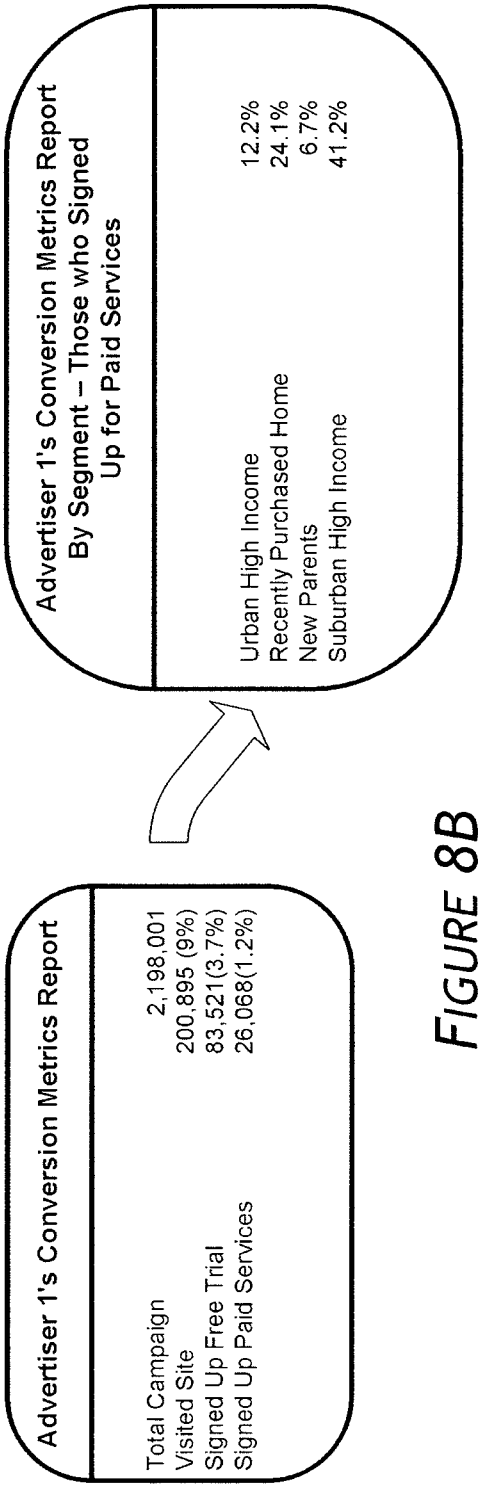


FIGURE 8B

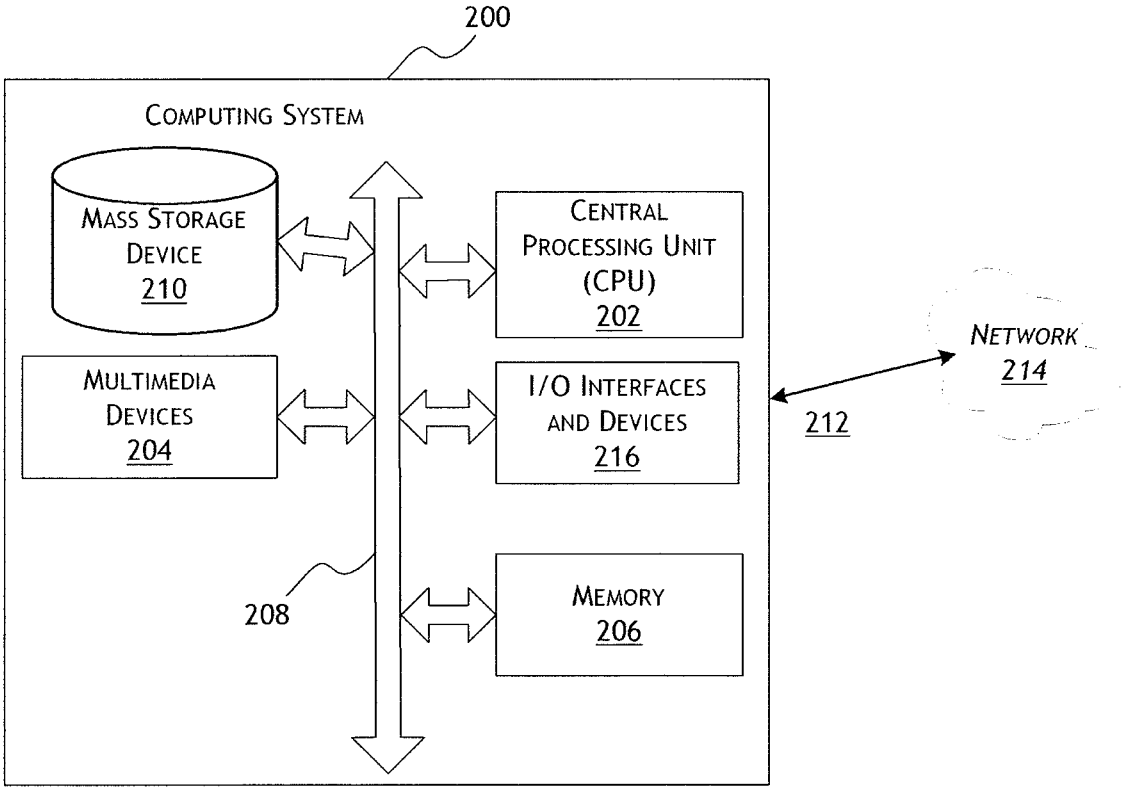

200
COMPUTING SYSTEM
MASS STORAGE DEVICE 210
CENTRAL PROCESSING UNIT (CPU) 202
MULTIMEDIA DEVICES 204
I/O INTERFACES AND DEVICES 216
MEMORY 206
208
212
NETWORK 214

FIGURE 9