Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 2873128 C 2022/10/18

(11)(21) 2 873 128

(12) BREVET CANADIEN
CANADIAN PATENT

(13) C

(86) Date de dépôt PCT/PCT Filing Date: 2013/08/28
(87) Date publication PCT/PCT Publication Date: 2014/03/06
(45) Date de délivrance/Issue Date: 2022/10/18
(85) Entrée phase nationale/National Entry: 2014/12/02
(86) N° demande PCT/PCT Application No.: US 2013/057045
(87) N° publication PCT/PCT Publication No.: 2014/036119
(30) Priorités/Priorities: 2012/08/30 (US61/695,169); 2012/09/06 (US61/697,597); 2013/04/12 (AU2013204953)

(51) Cl.Int./Int.Cl. *G06F 17/00* (2019.01), *G06F 16/951* (2019.01), *G06F 16/9535* (2019.01), *G06F 21/62* (2013.01), *H04L 12/16* (2006.01), *H04L 51/52* (2022.01), *H04L 9/32* (2006.01), *H04W 4/12* (2009.01), *H04W 4/21* (2018.01)

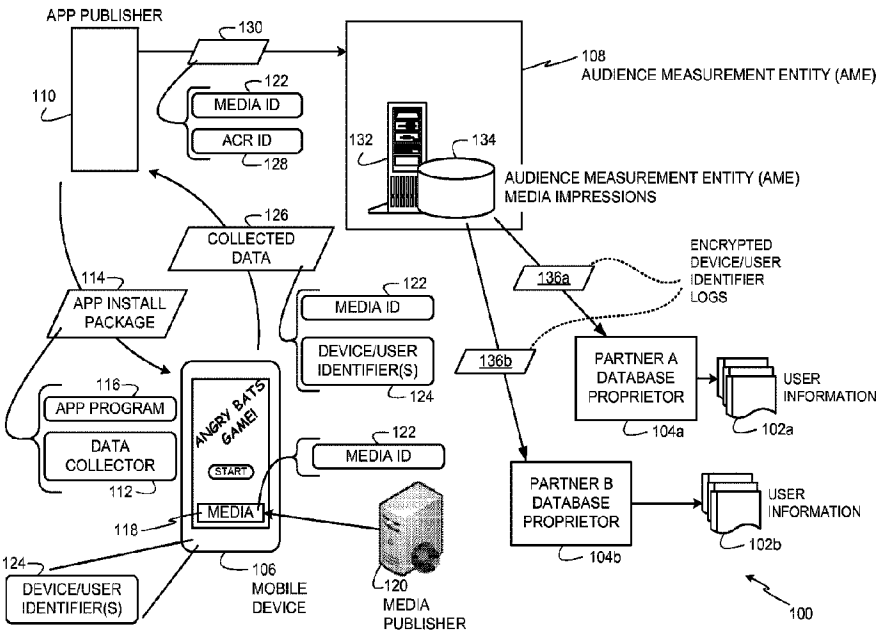
(72) Inventeurs/Inventors:
BURBANK, JOHN R., US;
ALLA, MADHUSUDHAN REDDY, US

(73) Propriétaire/Owner:
THE NIELSEN COMPANY (US), LLC, US

(74) Agent: ROWAND LLP

(54) Titre : PROCEDE ET APPAREIL POUR RECUEILLIR DES INFORMATIONS D'UTILISATEUR REPARTIES POUR IMPRESSION MEDIA ET TERMES DE RECHERCHE

(54) Title: METHODS AND APPARATUS TO COLLECT DISTRIBUTED USER INFORMATION FOR MEDIA IMPRESSIONS AND SEARCH TERMS



(57) Abrégé/Abstract:
Disclosed examples involve decoding information from a mobile device into a plurality of encrypted identifiers identifying at least one of the mobile device or a user of the mobile device, sending ones of the encrypted identifiers to corresponding database proprietors, receiving a plurality of user information corresponding to the ones of the encrypted identifiers from the corresponding database proprietors, and associating the plurality of user information with at least one of a search term collected at the mobile device or a media impression logged for media presented at the mobile device.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 March 2014 (06.03.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/036119 A1

(51) International Patent Classification:
G06F 17/00 (2006.01) *G06F 17/30* (2006.01)

(21) International Application Number:
PCT/US2013/057045

(22) International Filing Date:
28 August 2013 (28.08.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/695,169 30 August 2012 (30.08.2012) US
61/697,597 6 September 2012 (06.09.2012) US
2013204953 12 April 2013 (12.04.2013) AU

(71) Applicant *(for all designated States except SA, US)*: **THE NIELSEN COMPANY (US), LLC** [US/US]; 150 North Martingale Road, Schaumburg, Illinois 60173 (US).

(72) Inventors; and
(71) Applicants *(for US only)*: **BURBANK, John R.** [US/US]; 770 Broadway, New York, New York 10003 (US). **ALLA, Madhusudhan Reddy** [IN/US]; 1515 Evanvale Dr., Allen, Texas 75013 (US).

(74) Agent: **HERNANDEZ, Felipe**; Hanley, Flight & Zimmerman, LLC, 150 S. Wacker Drive, Suite 2100, Chicago, Illinois 60606 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, 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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) **Title**: METHODS AND APPARATUS TO COLLECT DISTRIBUTED USER INFORMATION FOR MEDIA IMPRESSIONS AND SEARCH TERMS

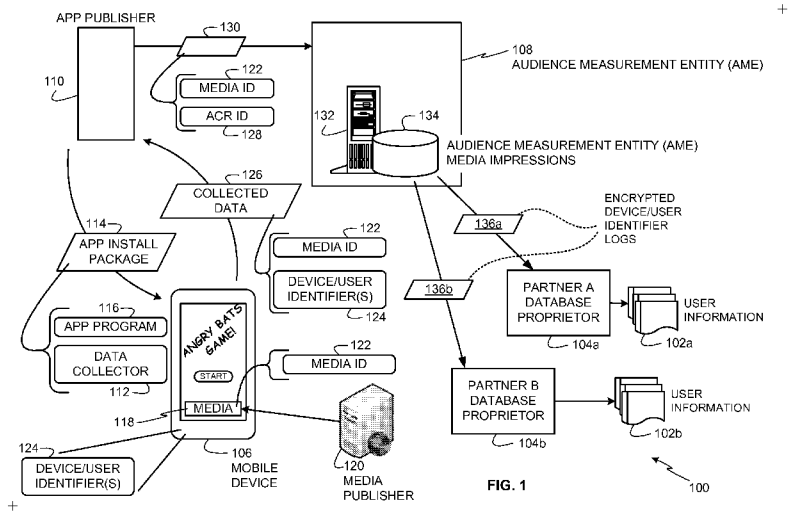


FIG. 1

(57) **Abstract**: Disclosed examples involve decoding information from a mobile device into a plurality of encrypted identifiers identifying at least one of the mobile device or a user of the mobile device, sending ones of the encrypted identifiers to corresponding database proprietors, receiving a plurality of user information corresponding to the ones of the encrypted identifiers from the corresponding database proprietors, and associating the plurality of user information with at least one of a search term collected at the mobile device or a media impression logged for media presented at the mobile device.

WO 2014/036119 A1

METHODS AND APPARATUS TO COLLECT DISTRIBUTED USER INFORMATION FOR MEDIA IMPRESSIONS AND SEARCH TERMS

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates generally to monitoring media and, more particularly, to methods and apparatus to collect distributed user information for media impressions and search terms.

BACKGROUND

[0003] Traditionally, audience measurement entities determine audience engagement levels for media programming based on registered panel members. That is, an audience measurement entity enrolls people who consent to being monitored into a panel. The audience measurement entity then monitors those panel members to determine media programs (e.g., television programs or radio programs, movies, DVDs, etc.) exposed to those panel members. In this manner, the audience measurement entity can determine exposure measures for different media content based on the collected media measurement data.

[0004] Techniques for monitoring user access to Internet resources such as web pages, advertisements and/or other content has evolved significantly over the years. Some known systems perform such monitoring primarily through server logs. In particular, entities serving content on the Internet can use known techniques to log the number of requests received for their content at their server.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] FIG. 1 depicts an example system to collect user information from distributed database proprietors for associating with impressions of media presented at mobile devices.

[0006] FIG. 2 depicts an example apparatus to encrypt device and/or user identifiers, and encode the encrypted device and/or user identifiers into an application campaign rating (ACR) identifier.

[0007] FIG. 3 depicts an example apparatus to decode encrypted device and/or user identifiers from the ACR identifier of FIG. 2, and send the encrypted device and/or user identifiers to corresponding database proprietors to request user information associated with the encrypted device and/or user identifiers.

[0008] FIG. 4 depicts the example apparatus of FIG. 3 decoding an ACR identifier having some empty fields that do not contain any device and/or user identifiers.

[0009] FIG. 5 is a flow diagram representative of example machine readable instructions that may be executed to collect media identifiers and device and/or user identifiers at mobile devices.

[0010] FIG. 6 is a flow diagram representative of example machine readable instructions that may be executed to encrypt device and/or user identifiers, and encode the encrypted device and/or user identifiers into the ACR identifier of FIG. 2.

[0011] FIG. 7 is a flow diagram representative of example machine readable instructions that may be executed to decode encrypted device and/or user identifiers from the ACR identifier of FIG. 2, and collect user information associated with the encrypted device and/or user identifiers from corresponding database proprietors.

[0012] FIG. 8 is an example processor system that may be used to execute the example instructions of FIGS. 5-7, 11, and 15 to implement example apparatus and systems disclosed herein.

[0013] FIG. 9 depicts another example system to collect user information from distributed database proprietors for associating with impressions of media presented at mobile devices.

[0014] FIG. 10 depicts yet another example system to collect user information from distributed database proprietors for associating with impressions of media presented at mobile devices.

[0015] FIG. 11 is a flow diagram representative of example machine readable instructions that may be executed to collect media identifiers and device and/or user identifiers at a media publisher.

[0016] FIG. 12 is an example system to collect user information from distributed database proprietors for associating with search terms provided by users at mobile devices.

[0017] FIG. 13 depicts another example system to collect user information from distributed database proprietors for associating with search terms provided by users at mobile devices.

[0018] FIG. 14 depicts yet another example system to collect user information from distributed database proprietors for associating with search terms provided by users at mobile devices.

[0019] FIG. 15 is a flow diagram representative of example machine readable instructions that may be executed to collect search terms and device and/or user identifiers at a search provider.

DETAILED DESCRIPTION

[0020] Techniques for monitoring user access to Internet resources such as web pages, advertisements and/or other content has evolved significantly over the years. At one point in the past, such monitoring was done primarily through server logs. In particular, entities serving content on the Internet would log the number of requests received for their content at their server. Basing Internet usage research on server logs is problematic for several reasons. For example, server logs can be tampered with either directly or via zombie programs which repeatedly request content from the server to increase the server log counts. Secondly, content is sometimes retrieved once, cached locally and then repeatedly viewed from the local cache without involving the server in the repeat viewings. Server logs cannot track these views of cached content. Thus, server logs are susceptible to both over-counting and under-counting errors.

[0021] The inventions disclosed in Blumenau, US Patent 6,108,637, fundamentally changed the way Internet monitoring is performed and overcame the limitations of the server side log monitoring techniques described above. For example, Blumenau disclosed a technique wherein Internet content to be tracked is tagged with beacon instructions. In particular, monitoring instructions are associated with the HTML of the content to be tracked. When a client requests the content, both the content and the beacon instructions are downloaded to the client. The beacon instructions are, thus, executed whenever the content is accessed, be it from a server or from a cache.

[0022] The beacon instructions cause monitoring data reflecting information about the access to the content to be sent from the client that downloaded the content to a monitoring entity. Typically, the monitoring entity is an audience measurement entity

that did not provide the content to the client and who is a trusted third party for providing accurate usage statistics (e.g., The Nielsen Company, LLC). Advantageously, because the beaconing instructions are associated with the content and executed by the client browser whenever the content is accessed, the monitoring information is provided to the audience measurement company irrespective of whether the client is a panelist of the audience measurement company.

[0023] It is useful, however, to link demographics and/or other user information to the monitoring information. To address this issue, the audience measurement company establishes a panel of users who have agreed to provide their demographic information and to have their Internet browsing activities monitored. When an individual joins the panel, they provide detailed information concerning their identity and demographics (e.g., gender, race, income, home location, occupation, etc.) to the audience measurement company. The audience measurement entity sets a cookie on the panelist computer that enables the audience measurement entity to identify the panelist whenever the panelist accesses tagged content and, thus, sends monitoring information to the audience measurement entity.

[0024] Since most of the clients providing monitoring information from the tagged pages are not panelists and, thus, are unknown to the audience measurement entity, it is necessary to use statistical methods to impute demographic information based on the data collected for panelists to the larger population of users providing data for the tagged content. However, panel sizes of audience measurement entities remain small compared to the general population of users. Thus, a problem is presented as to how to increase panel sizes while ensuring the demographics data of the panel is accurate.

[0025] There are many database proprietors operating on the Internet. These database proprietors provide services to large numbers of subscribers. In exchange for the provision of the service, the subscribers register with the proprietor. As part of this registration, the subscribers provide detailed demographic information. Examples of such database proprietors include social network providers such as Facebook, Myspace, etc. These database proprietors set cookies on the computers of their subscribers to enable the database proprietor to recognize the user when they visit their website.

[0026] The protocols of the Internet make cookies inaccessible outside of the domain (e.g., Internet domain, domain name, etc.) on which they were set. Thus, a

cookie set in the amazon.com domain is accessible to servers in the amazon.com domain, but not to servers outside that domain. Therefore, although an audience measurement entity might find it advantageous to access the cookies set by the database proprietors, they are unable to do so. In addition, apps that run on mobile device platforms do not use cookies in the same way as web browsers. Although apps do present media that is worthy of impression tracking, prior techniques that use cookie-based approaches for tracking such media impressions are unusable in the app environment context.

[0027] In view of the foregoing, an audience measurement company would like to leverage the existing databases of database proprietors to collect more extensive Internet usage and demographic data and/or user data for associating with media impressions tracked on devices that execute apps that do not employ cookies which are more commonly used in web browsers. However, the audience measurement entity is faced with several problems in accomplishing this end. For example, a problem is presented as to how to access the data of the database proprietors without compromising the privacy of the subscribers, the panelists, or the proprietors of the tracked content. Another problem is how to access this data given the technical restrictions imposed by app software platforms of mobile devices that do not employ cookies.

[0028] Example methods, apparatus and/or articles of manufacture disclosed herein enable tracking media impressions for media presented by mobile device apps that execute on mobile devices, without needing to rely on cookies to track such media impressions. In this manner, an audience measurement entity (AME) can track media impressions on mobile devices on which apps that do not employ cookies have higher usage rates than web browsers that do employ cookies. Examples disclosed herein also protect privacies of users by encrypting identification information in such a way that personally-identifying information is not revealed to the AME. Examples disclosed herein accomplish this by using an application campaign rating (ACR) identifier (ID) that includes one or more encrypted device and/or user identifier(s) (i.e., device/user identifier(s)) retrieved from a mobile device. The one or more encrypted device/user identifier(s) can then be used to retrieve user information for a user of the mobile device by sending the one or more encrypted device/user identifier(s) to one or more corresponding database proprietors that store user information for its registered users. In the illustrated examples, to protect users' privacies, the AME

does not have keys to decrypt the encrypted device/user identifiers, and each database proprietor has only its respective key(s) useable to decrypt only device/user identifier(s) pertaining to its services (e.g., wireless carrier services, social networking services, email services, mobile phone ecosystem app or media services, etc.). In this manner, personally-identifying information for particular services will not be revealed to the AME or to just any database proprietor, but only to the database proprietor that provides the particular service.

[0029] In examples disclosed herein, when an audience measurement entity receives an ACR ID including one or more encrypted device/user identifier(s), the audience measurement entity can request user information from one or more partnered database proprietors for the encrypted device/user identifier(s). In this manner, the partnered database proprietor(s) can provide user information to the audience measurement entity for the encrypted device/user identifier(s), and associate the user information with one or more media ID's of media presented by app(s) on one or more mobile device(s). Because the identification of users or client mobile devices is done with reference to enormous databases of users far beyond the quantity of persons present in a conventional audience measurement panel, the data developed from this process is extremely accurate, reliable and detailed. In some examples, by agreeing to participate in concerted audience measurement efforts, the partnered database proprietors are provided with audience user information and exposure information collected by other partnered database proprietors. In this manner, partnered database proprietors can supplement their own audience exposure metrics with information provided by other partnered database proprietors.

[0030] Example methods, apparatus, and articles of manufacture disclosed herein can be used to determine content impressions, advertisement impressions, content exposure, and/or advertisement exposure using user information, which is distributed across different databases (e.g., different website owners, service providers, etc.) on the Internet. Not only do example methods, apparatus, and articles of manufacture disclosed herein enable more accurate correlation of Internet media exposure to user information, but they also effectively extend panel sizes and compositions beyond persons participating in the panel of an audience measurement entity and/or a ratings entity to persons registered in other Internet databases such as the databases of wireless service carriers, mobile software/service providers, social medium sites (e.g., Facebook, Twitter, Google, etc.), and/or any other Internet sites such as Yahoo!,

MSN, Apple iTunes, Experian, etc. This extension effectively leverages the media impression tracking capabilities of the audience measurement entity and the use of databases of non-AME entities such as social media and other websites to create an enormous, demographically accurate panel that results in accurate, reliable measurements of exposures to Internet content such as advertising and/or programming.

[0031] Traditionally, audience measurement entities (also referred to herein as "ratings entities") determine demographic reach for advertising and media programming based on registered panel members. That is, an audience measurement entity enrolls people that consent to being monitored into a panel. During enrollment, the audience measurement entity receives demographic information from the enrolling people so that subsequent correlations may be made between advertisement/media exposure to those panelists and different demographic markets. Unlike traditional techniques in which audience measurement entities rely solely on their own panel member data to collect demographics-based audience measurement, example methods, apparatus, and/or articles of manufacture disclosed herein enable an audience measurement entity to share demographic information with other entities that operate based on user registration models. As used herein, a user registration model is a model in which users subscribe to services of those entities by creating an account and providing demographic-related information about themselves. Sharing of demographic information associated with registered users of database proprietors enables an audience measurement entity to extend or supplement their panel data with substantially reliable demographics information from external sources (e.g., database proprietors), thus extending the coverage, accuracy, and/or completeness of their demographics-based audience measurements. Such access also enables the audience measurement entity to monitor persons who would not otherwise have joined an audience measurement panel. Any entity having a database identifying demographics of a set of individuals may cooperate with the audience measurement entity. Such entities may be referred to as "database proprietors" and include entities such as wireless service carriers, mobile software/service providers, social medium sites (e.g., Facebook, Twitter, Google, etc.), and/or any other Internet sites such as Yahoo!, MSN, Apple iTunes, Experian, etc.

[0032] Example methods, apparatus, and/or articles of manufacture disclosed herein may be implemented by an audience measurement entity (e.g., any entity interested in measuring or tracking audience exposures to advertisements, content, and/or any other media) in cooperation with any number of database proprietors such as online web services providers to develop online media exposure metrics. Such database proprietors/online web services providers may be wireless service carriers, mobile software/service providers, social network sites (e.g., Facebook, Twitter, MySpace, etc.), multi-service sites (e.g., Yahoo!, Google, Experian, etc.), online retailer sites (e.g., Amazon.com, Buy.com, etc.), and/or any other web service(s) site that maintains user registration records.

[0033] In some examples, to increase the likelihood that measured viewership is accurately attributed to the correct demographics, example methods, apparatus, and/or articles of manufacture disclosed herein use user information located in the audience measurement entity's records as well as user information located at one or more database proprietors (e.g., web service providers) that maintain records or profiles of users having accounts therewith. In this manner, example methods, apparatus, and/or articles of manufacture disclosed herein may be used to supplement user information maintained by a ratings entity (e.g., an audience measurement company such as The Nielsen Company of Schaumburg, Illinois, United States of America, that collects media exposure measurements, demographics, and/or other user information) with user information from one or more different database proprietors (e.g., web service providers).

[0034] The use of demographic information from disparate data sources (e.g., high-quality demographic information from the panels of an audience measurement company and/or registered user data of web service providers) results in improved reporting effectiveness of metrics for both online and offline advertising campaigns. Example techniques disclosed herein use online registration data to identify demographics of users, and/or other user information, and use server impression counts, and/or other techniques to track quantities of impressions attributable to those users. Online web service providers such as wireless service carriers, mobile software/service providers, social network sites (e.g., Facebook, Twitter, MySpace, etc.), multi-service sites (e.g., Yahoo!, Google, Experian, etc.), online retailer sites (e.g., Amazon.com, Buy.com, etc.), etc. (collectively and individually referred to herein as online database proprietors) maintain detailed demographic information (e.g., age,

gender, geographic location, race, income level, education level, religion, etc.) collected via user registration processes. An impression corresponds to a home or individual having been exposed to the corresponding media content and/or advertisement. Thus, an impression represents a home or an individual having been exposed to an advertisement or content or group of advertisements or content. In Internet advertising, a quantity of impressions or impression count is the total number of times an advertisement or advertisement campaign has been accessed by a web population (e.g., including number of times accessed as decreased by, for example, pop-up blockers and/or increased by, for example, retrieval from local cache memory).

[0035] FIG. 1 depicts an example system 100 to collect user information (e.g., user information 102a and 102b) from distributed database proprietors 104a and 104b for associating with impressions of media presented at a mobile device 106. In the illustrated examples, user information or user data includes one or more of demographic data, purchase data, and/or other data indicative of user activities, behaviors, and/or preferences related to information accessed via the Internet, purchases, media accessed on electronic devices, physical locations (e.g., retail or commercial establishments, restaurants, venues, etc.) visited by users, etc. Examples disclosed herein are described in connection with a mobile device, which may be a mobile phone, a mobile communication device, a tablet, a gaming device, a portable media presentation device, etc. However, examples disclosed herein may be implemented in connection with non-mobile devices such as internet appliances, smart televisions, internet terminals, computers, or any other device capable of presenting media received via network communications.

[0036] In the illustrated example of FIG. 1, to track media impressions on the mobile device 106, an audience measurement entity (AME) 108 partners with or cooperates with an app publisher 110 to download and install a data collector 112 on the mobile device 106. The app publisher 110 of the illustrated example may be a software app developer that develops and distributes apps to mobile devices and/or a distributor that receives apps from software app developers and distributes the apps to mobile devices. In the illustrated example, to download and install the data collector 112 on the mobile device 106, the app publisher 110 downloads an app install package 114 to the mobile device 106 when the mobile device 106 requests a purchased or free app program 116. The app publisher 110 locates the requested

app program 116 and the data collector 112 in the app install package 114, and then it sends the app install package 114 to the mobile device 106 for installing the app program 116 and the data collector 112. In some examples, the app publisher 110 may first obtain the consent of a user of the mobile device 106 to participate in a media tracking program before sending the data collector 112 for installation on the mobile device 106.

[0037] In the illustrated example, the app program 116 is a game entitled "Angry Bats" that presents media 118 received from a media publisher 120. The media 118 may be an advertisement, video, audio, text, a graphic, a web page, news, educational media, entertainment media, or any other type of media. In the illustrated example, a media ID 122 is provided in the media 118 to enable identifying the media 118 so that the AME 108 can credit the media 118 with media impressions when the media 118 is presented on the mobile device 106 or any other device that is monitored by the AME 108.

[0038] In the illustrated example, the AME 108 provides the data collector 112 to the app publisher 110 for packaging with the app program 116 in the app install package 114. In some examples, the app publisher 110 provides the data collector 112 as a program separate from the app program 116. In other examples, the app publisher 110 compiles or otherwise includes the data collector 112 in the app program 116 rather than installing the data collector 112 as a program separate from the app program 116. The data collector 112 of the illustrated example includes instructions (e.g., Java, java script, or any other computer language or script) that, when executed by the mobile device 106, cause the mobile device 106 to collect the media ID 122 of the media 118 presented by the app program 116 and/or the mobile device 106, and to collect one or more device/user identifier(s) 124 stored in the mobile device 106. The device/user identifier(s) 124 of the illustrated example include identifiers that can be used by corresponding ones of the partner database proprietors 104a-b to identify the user or users of the mobile device 106, and to locate user information 102a-b corresponding to the user(s). For example, the device/user identifier(s) 124 may include hardware identifiers (e.g., an international mobile equipment identity (IMEI), a mobile equipment identifier (MEID), a media access control (MAC) address, etc.), an app store identifier (e.g., a Google Android ID, an Apple ID, an Amazon ID, etc.), an open source unique device identifier (OpenUDID), an open device identification number (ODIN), a login identifier (e.g., a username), an

email address, user agent data (e.g., application type, operating system, software vendor, software revision, etc.), third-party service identifiers (e.g., advertising service identifiers, device usage analytics service identifiers, demographics collection service identifiers), etc. In some examples, fewer or more device/user identifier(s) 124 may be used. In addition, although only two partner database proprietors 104a-b are shown in FIG.1, the AME 108 may partner with any number of partner database proprietors to collect distributed user information (e.g., the user information 102a-b).

[0039] In some examples, the types of device/user identifiers 124 are different from device to device depending on the type of device, the manufacturer of the device, the software installed on the device, etc. For example, a mobile device having cellular 2G, 3G, and/or 4G capabilities will have an assigned IMEI number. However, a mobile device capable of Wi-Fi, but not having cellular communication capabilities, will not have an IMEI number. As such, one or more other parameter(s) of the Wi-Fi mobile device may be used as the device/user identifiers 124. Such other parameters may include, for example, a MAC address, a login ID, or any other identifier or information available to the Wi-Fi capable device and that is not specific to cellular communications.

[0040] By being able to select or access multiple different types of device/user identifiers 124, the AME 108 increases the opportunities for collecting corresponding user information. For example, the AME 108 is not tied to requesting user information from a single source (e.g., only one of the partner database proprietors 104a-b). Instead, the AME 108 can leverage relationships with multiple partner database proprietors (e.g., the partner database proprietors 104a-b). If one or some partner database proprietors are unable or become unwilling to share user data, the AME 108 can request the user data from one or more other partner database proprietor(s).

[0041] In some examples, the mobile device 106 may not allow access to identification information stored in the mobile device 106. For such instances, the disclosed examples enable the AME 108 to store an AME-provided identifier (e.g., an identifier managed and tracked by the AME 108) in the mobile device 106 to track media impressions on the mobile device 106. For example, the AME 108 may provide instructions in the data collector 112 to set an AME-provided identifier in memory space accessible by and/or allocated to the app program 116, and the data collector 112 uses the identifier as a device/user identifier 124. In such examples, the AME-provided identifier set by the data collector 112 persists in the memory space

even when the app program 116 and the data collector 112 are not running. In this manner, the same AME-provided identifier can remain associated with the mobile device 106 for extended durations. In some examples in which the data collector 112 sets an identifier in the mobile device 106, the AME 108 may recruit a user of the mobile device 106 as a panelist, and may store user information collected from the user during a panelist registration process and/or collected by monitoring user activities/behavior via the mobile device 106 and/or any other device used by the user and monitored by the AME 108. In this manner, the AME 108 can associate user information of the user (from panelist data stored by the AME 108) with media impressions attributed to the user on the mobile device 106.

[0042] In the illustrated example, the data collector 112 sends the media ID 122 and the one or more device/user identifier(s) 124 as collected data 126 to the app publisher 110. Alternatively, the data collector 112 may be configured to send the collected data 126 to another collection entity (other than the app publisher 110) that has been contracted by the AME 108 or is partnered with the AME 108 to collect media ID's (e.g., the media ID 122) and device/user identifiers (e.g., the device/user identifier(s) 124) from mobile devices (e.g., the mobile device 106). In the illustrated example, the app publisher 110 (or a collection entity) generates an ACR ID 128 that includes the device/user identifier(s) 124, and the app publisher (or a collection entity) sends the media ID 122 and the ACR ID 128 as impression data 130 to a server 132 at the AME 108. The impression data 130 of the illustrated example may include one media ID 122 and one ACR ID 128 to report a single impression of the media 118, or it may include numerous media ID's and ACR ID's based on numerous instances of collected data (e.g., the collected data 126) received from the mobile device 106 and/or other mobile devices to report multiple impressions of media. In the illustrated example, the server 130 of the illustrated example stores the impression data 130 in an AME media impressions store 134 (e.g., a database or other data structure). Subsequently, the AME 108 sends the device/user identifier(s) 124 from the ACR ID 128 to corresponding partner database proprietors (e.g., the partner database proprietors 104a-b) to receive user information (e.g., the user information 102a-b) corresponding to the device/user identifier(s) 124 from the partner database proprietors so that the AME 108 can associate the user information with corresponding media impressions of media (e.g., the media 118) presented at mobile devices (e.g., the mobile device 106).

[0043] Although the above description describes the app publisher 110 (or other collection entity) as generating the ACR ID 128, in other examples, the data collector 112 at the mobile device 106 generates the ACR ID 128 that includes the device/user identifier(s) 124. In such examples, the data collector 112 sends the ACR ID 128 to the app publisher 110 (or other collection entity) in the collected data 126.

[0044] In the illustrated example, to protect the privacy of the user of the mobile device 106, the device/user identifier(s) 124 is/are encrypted before sending it/them to the AME 108 in the ACR ID 128. In the illustrated examples, the encryption process is performed so that neither the app publisher (110) (or other collection entity) nor the AME 108, or any other intermediate entity, can access the device/user identifier(s) 124 before they are sent to corresponding partner database proprietors (e.g., the partner database proprietors 104a-b). To encrypt the device/user identifier(s) 124, each partner database proprietor (e.g., the partner database proprietors 104a-b) for which identification information can be retrieved from the mobile device 106 is provided with one or more encryption keys specific to that partner database proprietor. In this manner, each partner database proprietor has a different set of keys so that each partner database proprietor can only recover one or more of the device/user identifier(s) 124 that pertain(s) to it. For example, a wireless service carrier can only retrieve an IMEI or MEID number, a social network site can only retrieve a login username corresponding to its social network services, etc. Copies of the one or more encryption keys can be provided to the app publisher 110 in an encryption algorithm (e.g., an SSH-1 encryption algorithm). In the illustrated example, the AME 108 provides the encryption algorithm and the encryption keys to the app publisher 110 as an encryption software package or bundle (e.g., an encryptor 202 of FIG. 2) from which the app publisher 110 cannot recover or extract the encryption keys. In this manner, the app publisher 110 is not able to access the device/user identifier(s) 124. In other examples, the app publisher 110 is able to access the device/user identifier(s) 124 if authorized by a user of the mobile device 106 (e.g., during installation of the app program 116). In such examples, the app publisher 110 may still encrypt the device/user identifier(s) 124 before sending them to the AME 108.

[0045] In the illustrated examples, the encryption algorithm is also provided with partner database proprietor identifiers along with corresponding ones of the encryption keys for each of the partner database proprietors (e.g., the partner

database proprietors 104a-b). When encrypting the device/user identifier(s) 124, the encryption algorithm can append, prepend, concatenate, or otherwise associate corresponding partner database proprietor identifiers to or with the encrypted device/user identifier(s) (e.g., encrypted device/user identifier(s) 208a-b of FIG. 2) so that the AME 108 can access the partner database proprietor identifiers, without decrypting the encrypted device/user identifier(s), to identify which of the encrypted device/user identifier(s) corresponds to which partner database proprietor. In this manner, the AME 108 can deliver the encrypted device/user identifier(s) to corresponding partner database proprietor(s) even though it cannot decrypt the device/user identifier(s) 124.

[0046] In some examples, the app publisher 110 can run the encryption software at one of its servers or computers that receives the collected data 126 from the mobile device 106. In such examples, the media ID 122 and the device/user identifier(s) 124 are sent by the mobile device 106 as the collected data 126 via a secure connection between the encryption software running at the app publisher 110 and the mobile device 106. In this manner, the device/user identifier(s) 124 is/are not intercepted by the app publisher 110 before they are encrypted using the encryption keys corresponding to the different database proprietors.

[0047] In other examples, the encryption software to encrypt the device/user identifier(s) 124 is provided in the data collector 112 so that the data collector 112 can encrypt the device/user identifier(s) 124 at the mobile device 106 before sending encrypted device/user identifier(s) to the app publisher 110 (or other collection entity). In some examples in which the data collector 112 encrypts the device/user identifier(s) 124, the data collector 112 also encodes the encrypted device/user identifier(s) into an ACR ID (e.g., the ACR ID 128). In such examples, the data collector 112 sends the ACR ID 128 and the media ID 122 to the app publisher 110 (or other collection entity) in the collected data 126.

[0048] After the AME 108 receives the ACR ID 128 including the device/user identifier(s) 124 in encrypted format, the AME 108 sends encrypted device/user identifier logs 136a-b to corresponding partner database proprietors (e.g., the partner database proprietors 104a-b). In the illustrated example, each of the encrypted device/user identifier logs 136a-b may include a single encrypted device/user identifier, or it may include numerous aggregate encrypted device/user identifiers received over time from one or more mobile devices. After receiving the encrypted

device/user identifier logs 136a-b, each of the partner database proprietors 104a-b decrypts its respective encrypted device/user identifiers using its copy(ies) of the encryption key(s). The partner database proprietors 104a-b then look up their users corresponding to the decrypted device/user identifiers, and collect corresponding user information 102a-b for those users for sending to the AME 108. For example, if the partner database proprietor 104a is a wireless service provider, the encrypted device/user identifier log 136a includes IMEI numbers, and the wireless service provider accesses its subscriber records to find users having IMEI numbers matching the IMEI numbers received in the encrypted device/user identifier log 136a. When the users are identified, the wireless service provider copies the users' user information to the user information 102a for delivery to the AME 108.

[0049] FIG. 9 depicts another example system 900 to collect user information (e.g., the user information 102a and 102b) from distributed database proprietors 104a and 104b for associating with impressions of media presented at the mobile device 106. In the illustrated example of FIG. 9, like reference numbers are used to refer to the same or similar components as described above in connection with FIG. 1. In the illustrated example of FIG. 9, a data collector 912 is shown as being located in the app program 116. For example, the data collector 912 may include instructions coded in the app program 116 to collect data in the mobile device 106. Alternatively, the data collector 912 may be a separate program downloaded separate from the app program 116 as part of the app install package 114 from the app publisher 110.

[0050] In the illustrated example of FIG. 9, the data collector 912 is configured to collect the device/user identifier(s) 124 from the mobile device 106. The example data collector 912 sends the device/user identifier(s) 124 to the app publisher 110 in the collected data 126, and it also sends the device/user identifier(s) 124 to the media publisher 120. The data collector 912 of the illustrated example does not collect the media ID 122 from the media 118 at the mobile device 106 as the data collector 112 does in the example system 100 of FIG. 1. Instead, the media publisher 120 that publishes the media 118 to the mobile device 106 retrieves the media ID 122 from the media 118 that it publishes. The media publisher 120 then associates the media ID 122 to the device/user identifier(s) 124 of the mobile device 106, and sends collected data 902 to the app publisher 110 that includes the media ID 122 and the associated device/user identifier(s) 124 of the mobile device 106. For example, when the media publisher 120 sends the media 118 to the mobile device 106, it does so by identifying

the mobile device 106 as a destination device for the media 118 using one or more of the device/user identifier(s) 124. In this manner, the media publisher 120 can associate the media ID 122 of the media 118 with the device/user identifier(s) 124 of the mobile device 106 indicating that the media 118 was sent to the particular mobile device 106 for presentation (e.g., to generate an impression of the media 118).

[0051] In the illustrated example, the app publisher 110 matches the device/user identifier(s) 124 from the collected data 902 to the device/user identifier(s) 124 from the collected data 126 to determine that the media ID 122 corresponds to media (e.g., the media 118) presented on the mobile device 106 associated with the device/user identifier(s) 124. The app publisher 110 of the illustrated example also generates an ACR ID 128 based on the device/user identifier(s) 124 as disclosed herein. The app publisher 110 then sends the impression data 130, including the media ID 122 and the associated ACR ID 128, to the AME 108. The AME 108 can then send the encrypted device/user identifier logs 136a-b to the partner database proprietors 104a-b to request the user information 102a-b as described above in connection with FIG. 1.

[0052] FIG. 10 depicts yet another example system 1000 to collect user information (e.g., the user information 102a and 102b) from distributed database proprietors 104a and 104b for associating with impressions of media presented at the mobile device 106. In the illustrated example of FIG. 10, like reference numbers are used to refer to the same or similar components as described above in connection with FIG. 1. In the illustrated example of FIG. 10, a data collector 1012 is shown as being located in the app program 116. For example, the data collector 1012 may include instructions coded in the app program 116 to collect data in the mobile device 106. Alternatively, the data collector 1012 may be a separate program downloaded separate from the app program 116 as part of the app install package 114 from the app publisher 110.

[0053] In the illustrated example of FIG. 10, the data collector 1012 is configured to collect the device/user identifier(s) 124 from the mobile device 106. The example data collector 1012 sends the device/user identifier(s) 124 to the media publisher 120. The data collector 1012 of the illustrated example does not collect the media ID 122 from the media 118 at the mobile device 106 as the data collector 112 does in the example system 100 of FIG. 1. Instead, the media publisher 120 that publishes the media 118 to the mobile device 106 retrieves the media ID 122 from the media 118

that it publishes. The media publisher 120 then associates the media ID 122 to the device/user identifier(s) 124 of the mobile device 106, and generates the ACR ID 128 based on the device/user identifier(s) 124 as disclosed herein. The media publisher 120 then sends the media impression data 130, including the media ID 122 and the ACR ID 128, to the AME 108. For example, when the media publisher 120 sends the media 118 to the mobile device 106, it does so by identifying the mobile device 106 as a destination device for the media 118 using one or more of the device/user identifier(s) 124. In this manner, the media publisher 120 can associate the media ID 122 of the media 118 with the device/user identifier(s) 124 and the ACR ID 128 of the mobile device 106 indicating that the media 118 was sent to the particular mobile device 106 for presentation (e.g., to generate an impression of the media 118). In the illustrated example, after the AME 108 receives the impression data 130 from the media publisher 120, the AME 108 can then send the encrypted device/user identifier logs 136a-b to the partner database proprietors 104a-b to request the user information 102a-b as described above in connection with FIG. 1.

[0054] Although the media publisher 120 is shown separate from the app publisher 110 in FIGS. 1, 9, and 10, the app publisher 110 may implement at least some of the operations of the media publisher 120 to send the media 118 to the mobile device 106 for presentation. For example, advertisement, content, or other media providers may send media (e.g., the media 118) to the app publisher 110 for publishing to the mobile device 106 via, for example, the app program 116 when it is executing on the mobile device 106. In such examples, the app publisher 110 implements the operations described above as being performed by the media publisher 120.

[0055] In some examples, the media publisher 120 operates as a third-party media publisher relative to other traditional media publishers. In such examples, the media publisher 120 receives media from media providers and/or other traditional media publishers for publishing to electronic devices (e.g., the mobile device 106) while tracking media impressions of the published media (e.g., the media 118) and/or identities of devices to which media is published. That is, in addition to performing traditional media publisher services of publishing media to electronic devices, the media publisher 120 of the illustrated example additionally collects media impression tracking information as discussed above in connection with FIGS. 9 and 10. Thus, in some examples, the media publisher 120 is a third party that is contracted by traditional media publishers to provide media impression tracking capabilities for

collecting media impressions and user information (e.g., the user information 102a-b) as disclosed herein.

[0056] In addition to associating user information (e.g., the user information 102a-b) with media IDs (e.g., the media ID 122) of published media, examples disclosed herein may additionally or alternatively be used to associate user information with other types of information collected from mobile devices representative of user interests and/or user behaviors. For example, techniques disclosed herein may also be used to monitor search terms provided by users at mobile devices, and associating those search terms with user information of users that provide the search terms. Example search terms may be provided via apps downloaded and installed on mobile devices, for searching information on the Internet and/or products at stores, websites, etc. For example, a search term may cause a search to be performed for information on the Internet, a search to be performed for a product, a search of a website to be performed, or a search for a website to be performed. Example systems that may be used to monitor search terms are described below in connection with FIGS. 12-14. In the illustrated examples of FIGS. 12-14, like reference numbers are used to refer to the same or similar components as described above in connection with FIG. 1.

[0057] FIG. 12 is an example system 1200 to collect user information (e.g., the user information 102a and 102b) from distributed database proprietors 104a-b for associating with search terms (e.g., search terms 1210) provided by users at mobile devices (e.g., the mobile device 106). In the illustrated example of FIG. 12, a data collector 1206 is shown as being located in an app program 1204 downloaded to the mobile device 106 in an app install package 1202 from the app publisher 110. For example, the data collector 1206 may include instructions coded in the app program 1204 to collect data in the mobile device 106. Alternatively, the data collector 1206 may be a separate program downloaded separate from the app program 1204 as part of the app install package 1202 from the app publisher 110.

[0058] In the illustrated example of FIG. 12, the app program 1204 provides search functionality so that users may search, for example, information on the Internet, products, services, etc. For example, when executing on the mobile device 106, the app program 1204 provides a search field 1208 for entering a search string including one or more search term(s) 1210. To provide the search functionality, the app program 1204 of the illustrated example sends the search term(s) 1210 to a search service provider 1212. In this manner, the search service provider 1212 can

perform the requested search, and return search results to the app program 1204 at the mobile device 106. In the illustrated example, the search service provider 1212 may be an Internet search engine (e.g., Google, Yahoo!, Bing, etc.), an Internet portal website, a retailer, etc.

[0059] When a user provides the search term(s) 1210 in the search field 1208, the data collector 1206 sends the search term(s) 1210, and the device/user identifier(s) 124 to the app publisher 110 as collected data 1214. The app publisher 110 can then generate the ACR ID 128 based on the device/user identifier(s) 124 using example techniques disclosed herein, and send the search term(s) 1210 and the ACR ID 128 to the AME 108 as user-interest data 1216. In other examples, the data collector 1206 may be configured to send the search term(s) 1210 and the ACR ID 128 (or the device/user identifier(s) 124) as the user-interest data 1216 directly to the AME 108. The AME 108 can then send the encrypted device/user identifier logs 136a-b to the partner database proprietors 104a-b to request the user information 102a-b as described above in connection with FIG. 1.

[0060] FIG. 13 depicts another example system 1300 to collect user information (e.g., the user information 102a and 102b) from distributed database proprietors 104a-b for associating with search terms (e.g., the search term(s) 1210) provided by users at mobile devices. In the illustrated example of FIG. 13, a data collector 1312 is shown as being located in the app program 1204. For example, the data collector 1312 may include instructions coded in the app program 1204 to collect data in the mobile device 106. Alternatively, the data collector 1312 may be a separate program downloaded separate from the app program 1204 as part of the app install package 1202 from the app publisher 110.

[0061] In the illustrated example of FIG. 9, the data collector 1312 is configured to collect the device/user identifier(s) 124 from the mobile device 106. The example data collector 1312 sends the device/user identifier(s) 124 to the app publisher 110 in the collected data 1214, and it also sends the device/user identifier(s) 124 to the search provider 1212. The data collector 1312 of the illustrated example does not collect the search terms 1210 from the search field 1208 at the mobile device 106 as the data collector 1206 does in the example system 1200 of FIG. 12. Instead, the search provider 1212 collects the search term(s) 1210 when received from the app program 1204. The search provider 1212 then associates the search term(s) 1210 with the device/user identifier(s) 124 of the mobile device 106, and sends collected

data 1302 to the app publisher 110 that includes the search term(s) 1210 and the associated device/user identifier(s) 124 of the mobile device 106. For example, when the search provider 1212 provides services to the mobile device 106, it does so by identifying the mobile device 106 using one or more of the device/user identifier(s) 124. In this manner, the search provider 1212 can associate the search term(s) 1210 with the device/user identifier(s) 124 of the mobile device 106 indicating which searches are performed for the particular mobile device 106.

[0062] In the illustrated example, the app publisher 110 matches the device/user identifier(s) 124 from the collected data 1302 to the device/user identifier(s) 124 from the collected data 126 to determine that the search term(s) 1210 correspond to a search provided for the mobile device 106 associated with the device/user identifier(s) 124. The app publisher 110 of the illustrated example also generates an ACR ID 128 based on the device/user identifier(s) 124 as disclosed herein. The app publisher 110 then sends the user-interest data 1216, including the search term(s) 1210 and the associated ACR ID 128, to the AME 108. The AME 108 can then send the encrypted device/user identifier logs 136a-b to the partner database proprietors 104a-b to request the user information 102a-b as described above in connection with FIG. 1.

[0063] FIG. 14 depicts yet another example system 1400 to collect user information (e.g., the user information 102a and 102b) from distributed database proprietors 104a and 104b for associating with the search term(s) 1210 provided at the mobile device 106. In the illustrated example of FIG. 14, a data collector 1412 is shown as being located in the app program 1204. For example, the data collector 1412 may include instructions coded in the app program 1204 to collect data in the mobile device 106. Alternatively, the data collector 1412 may be a separate program downloaded separate from the app program 1204 as part of the app install package 1202 from the app publisher 110.

[0064] In the illustrated example of FIG. 14, the data collector 1412 is configured to collect the device/user identifier(s) 124 from the mobile device 106. The example data collector 1412 sends the device/user identifier(s) 124 to the search provider 1212. The data collector 1412 of the illustrated example does not collect the search term(s) 1210 from the search field 1208 at the mobile device 106 as the data collector 1206 does in the example system 1200 of FIG. 12. Instead, the search provider 1212 retrieves the search term(s) 1210 when received from the app program 1205 executing on the mobile device 106. The search provider 1212 then associates the

search term(s) 1210 to the device/user identifier(s) 124 of the mobile device 106, and generates the ACR ID 128 based on the device/user identifier(s) 124 as disclosed herein. The search provider 1212 then sends the user-interest data 1216, including the search term(s) 1210 and the ACR ID 128, to the AME 108. For example, when the search provider 1212 provides search services to the mobile device 106, it does so by identifying the mobile device 106 using one or more of the device/user identifier(s) 124. In this manner, the search provider 1212 can associate the search term(s) 1210 with the device/user identifier(s) 124 and the ACR ID 128 of the mobile device 106 indicating that the search was performed for the particular mobile device 106. In other examples, the data collector 1412 at the mobile device 106 may be configured to send the search term(s) 1210 and the ACR ID 128 (or the device/user identifier(s) 124) as the user-interest data 1216 directly to the AME 108. In the illustrated example, after the AME 108 receives the user-interest data 1216 from the search provider 1212 (or from the mobile device 106), the AME 108 can then send the encrypted device/user identifier logs 136a-b to the partner database proprietors 104a-b to request the user information 102a-b as described above in connection with FIG. 1.

[0065] Although the search provider 1212 is shown separate from the app publisher 110 in FIGS. 1, 9, and 10, the app publisher 110 may implement at least some operations of the search provider 1212 to receive the search term(s) 1210 from the mobile device 106. For example, the data collector 1412 may send the search term(s) 1210 to the app publisher 110 so that the app publisher 110 may forward the search term(s) 1210 on to a search provider. In such examples, the app publisher 110 implements at least some of the operations described above as being performed by the search provider 1212.

[0066] FIG. 2 depicts an example apparatus 200 having an encryptor 202 to encrypt device and/or user identifiers (e.g., the device/user identifier(s) 124 of FIG. 1), and having an encoder 204 to encode the encrypted device and/or user identifiers into an application campaign rating (ACR) identifier (e.g., the ACR ID 128 of FIGS. 1, 9, 10, and 12-14). The encryptor 202 of the illustrated example is provided with encryption keys and partner database proprietor identifiers corresponding to the different partner database proprietors (e.g., partner database proprietors 104a-b of FIGS. 1, 9, 10, and 12-14) for which device/user identifiers 124 (FIGS. 1, 9, 10, and 12-14) can be collected from mobile devices. In the illustrated example, device

and/or user identifiers (e.g., the device/user identifier(s) 124 of FIGS. 1, 9, 10, and 12-14) include an IMEI/MEID number 124a, an Android ID 124b, a MAC address 124c, an OpenUDID 124d, an ODIN identifier 124e, a login ID 124f, user agent data 124g, a third-party 1 ID 124h, and a third-party 2 ID 124i. In the illustrated examples, the third-party 1 ID 124h and/or the third-party 2 ID 124i may be identifiers of targeted advertisement services, web analytics services, services that collect and store demographic information of users in association with unique identifiers (e.g., the third-party 1 ID 124h and/or the third-party 2 ID 124i) of those users. The encryptor 202 of the illustrated example uses corresponding encryption keys to encrypt the device/user identifiers 124 to corresponding encrypted device/user identifiers 208a-i. In addition, the encryptor 202 also provides (e.g., appends, prepends, or otherwise concatenates) corresponding partner database proprietor identifiers to corresponding ones of the encrypted device/user identifiers 208a-i so that the AME 108 can identify partner database proprietors (e.g., the partner database proprietors 104a-b of FIGS. 1, 9, 10, and 12-14) to which it should send corresponding ones of the encrypted device/user identifiers 208a-i. The encoder 204 of the illustrated example encodes the encrypted device/user identifiers 208a-i into the ACR ID 128. The ACR ID 128 is then sent to the AME 108.

[0067] The example apparatus 200 may be entirely or partially implemented at the mobile device 106 (FIGS. 1, 9, 10, and 12-14), entirely or partially implemented at the app publisher 110 (FIGS. 1, 9, 10, and 12-14) (or other collection entity), and/or entirely or partially implemented at the media publisher 120 (FIGS. 1, 9, and 10) (or search provider 1212 of FIGS. 12-14). In some examples, the encryptor 202 and the encoder 204 may both be implemented in the mobile device 106, to generate the ACR ID 128 and send the ACR ID 128 to the app publisher 110 (or other collection entity) in the collected data 126 along with the media ID 122 (and/or the search term(s) 1210). In other examples, the encryptor 202 may be implemented at the mobile device 106, and the encoder 204 may be implemented at the app publisher 110 (or other collection entity), at the media publisher 120, and/or at the search provider 1212. For example, the encryptor 202 may be provided in encryption software downloaded to the mobile device 106 as part of the data collector 112. In this manner, the encryptor 202 can encrypt the device/user identifier(s) 124 at the mobile device 106, and send the encrypted device/user identifier(s) 208a-i to the app publisher 110 (or other collection entity), to the media publisher 120, and/or to the

search provider 1212. The encoder 204 can then be used at the app publisher 110 (or other collection entity), at the media publisher 120, and/or at the search provider 1212 to generate the ACR ID 128 by encoding the encrypted device/user identifier(s) 208a-i into the ACR ID 128, and the app publisher 110 (or other collection entity), the media publisher 120, and/or the search provider 1212 sends the ACR ID 128 to the AME 108 along with the media ID 122 (e.g., as the impression data 130 of FIGS. 1, 9, and 10) or the search term(s) 1210 (e.g., as the user-interest data 1216).

[0068] In other examples, both of the encryptor 202 and the encoder 204 are implemented at the app publisher 110 (or other collection entity), at the media publisher 120, and/or at the search provider 1212. In such other examples, the app publisher 110 (or other collection entity), the media publisher 120, and/or the search provider 1212 receive(s) the device/user identifier(s) 124 from the mobile device 106. The app publisher 110 (or other collection entity), the media publisher 120, and/or the search provider 1212 generate(s) the ACR ID 128 to include the encrypted device/user identifier(s) 208a-i. The app publisher 110 (or other collection entity), the media publisher 120, and/or the search provider 1212 can then send the ACR ID 128 to the AME 108 along with the media ID 122 (e.g., as the impression data 130 of FIGS. 1, 9, and 10) or the search term(s) 1210 (e.g., as the user-interest data 1216 of FIGS. 12-14).

[0069] FIG. 3 depicts an example apparatus 300 to decode encrypted device and/or user identifiers 208a-i (FIG. 2) from the ACR ID 128 of FIGS. 1, 2, 9, 10, and 12-14, and send one or more of the encrypted device and/or user identifiers 208a-i to corresponding partner database proprietors 104a-e to request user information 102a-e associated with the encrypted device and/or user identifiers 208a-i. The apparatus 300 of the illustrated example includes a decoder 302 to decode the encrypted device and/or user identifiers 208a-i from the ACR ID 128. In the illustrated examples, the decoder 302 is implemented at the AME 108 of FIG. 1 (e.g., at the server 132 of the AME 108). The decoder 302 of the illustrated example determines which of the partner database proprietors 104a-e correspond to which of the encrypted device/user identifiers 208a-i based on, for example, partner database proprietor identifiers provided to the encrypted device/user identifiers 208a-i by the encryptor 202 of FIG. 2. The decoder 302 then sends corresponding ones of the encrypted device and/or user identifiers 208a-i to corresponding partner database proprietors 104a-e.

[0070] FIG. 4 depicts the example apparatus 300 of FIG. 3 decoding the ACR ID 128 in an example in which the ACR ID 128 has some empty fields that do not contain any encrypted device and/or user identifiers. In the illustrated example of FIG. 4, the decoder 302 decodes the encrypted device and/or user identifiers 208a and 208h which are located in the ACR ID 128, sends the encrypted device and/or user identifier 208a to the corresponding partner database proprietor 208a, and sends the encrypted device and/or user identifier 208h to the corresponding partner database proprietor 208h. Thus, although nine encrypted device and/or user identifiers 208a-i are shown in FIG. 3, in some examples, fewer (e.g., less than nine) encrypted device and/or user identifiers may be located in the ACR ID 128 such as in FIG. 4. In yet other examples, more than nine encrypted device and/or user identifiers may be encoded into the ACR ID 128.

[0071] While example manners of implementing the apparatus 200 and the apparatus 300 have been illustrated in FIGS. 2-4, one or more of the elements, processes and/or devices illustrated in FIGS. 2-4 may be combined, divided, re-arranged, omitted, eliminated and/or implemented in any other way. Further, the example encryptor 202, the example encoder 204, the example decoder 302 and/or, more generally, the example apparatus 200 and/or 300 may be implemented using hardware, software, firmware and/or any combination of hardware, software and/or firmware. Thus, for example, any of the example encryptor 202, the example encoder 204, the example decoder 302 and/or, more generally, the example apparatus 200 and/or 300 could be implemented using one or more analog or digital circuit(s), logical circuit(s), programmable processor(s), application specific integrated circuit(s) (ASIC(s)), programmable logic device(s) (PLD(s)) and/or field programmable logic device(s) (FPLD(s)), etc. When reading any of the apparatus or system claims of this patent to cover a purely software and/or firmware implementation, at least one of the example encryptor 202, the example encoder 204, and/or the example decoder 302 is/are hereby expressly defined to include a tangible computer readable storage device or storage disk such as a memory, a digital versatile disk (DVD), a compact disk (CD), a Blu-ray disk, etc. storing the software and/or firmware. Further still, the example apparatus 200 of FIG. 2 and/or the example apparatus 300 of FIGS. 3 and 4 may include one or more elements, processes and/or devices in addition to, or instead of, those illustrated in FIGS. 2-4, and/or may include more than one of any or all of the illustrated elements, processes and devices.

[0072] FIGS. 5, 11, 15, 6, and 7 are flow diagrams representative of machine readable instructions that may be executed to track media impressions and/or search terms and collect distributed user information for the media impressions and/or search terms using examples disclosed herein. In the examples of FIGS. 5, 11, 15, 6, and 7, operations and processes are shown that represent machine readable instructions comprising one or more programs for execution by one or more processors such as the processor 812 shown in the example computer 800 discussed below in connection with FIG. 8. The program(s) may be embodied in software stored on a tangible computer readable storage medium such as a CD-ROM, a floppy disk, a hard drive, a digital versatile disk (DVD), a Blu-ray disk, or a memory associated with the processor 812, but the entire program(s) and/or parts thereof could alternatively be executed by a device other than processor(s) such as the processor 812 and/or embodied in firmware or dedicated hardware. Further, although the example program(s) is/are disclosed herein with reference to the illustrated examples of FIGS. 5, 11, 15, 6, and 7, many other methods of implementing example apparatus 200 and 300 disclosed herein may alternatively be used. For example, the order of execution of the processes and/or operations may be changed, and/or some of the processes and/or operations disclosed herein may be changed, eliminated, or combined.

[0073] As mentioned above, example processes and/or operations of FIGS. 5, 11, 15, 6, and 7 may be implemented using coded instructions (e.g., computer and/or machine readable instructions) stored on a tangible computer readable storage medium such as a hard disk drive, a flash memory, a read-only memory (ROM), a compact disk (CD), a digital versatile disk (DVD), a cache, a random-access memory (RAM) and/or any other storage device or storage disk in which information is stored for any duration (e.g., for extended time periods, permanently, brief instances, for temporarily buffering, and/or for caching of the information). As used herein, the term tangible computer readable storage medium is expressly defined to include any type of computer readable storage device and/or storage disk and to exclude propagating signals and transmission media. As used herein, “tangible computer readable storage medium” and “tangible machine readable storage medium” are used interchangeably. Additionally or alternatively, the example processes and/or operations of FIGS. 5, 11, 15, 6, and 7 may be implemented using coded instructions (e.g., computer and/or machine readable instructions) stored on a non-transitory computer and/or machine readable medium such as a hard disk drive, a flash

memory, a read-only memory, a compact disk, a digital versatile disk, a cache, a random-access memory and/or any other storage device or storage disk in which information is stored for any duration (e.g., for extended time periods, permanently, for brief instances, for temporarily buffering, and/or for caching of the information). As used herein, the term non-transitory computer readable medium is expressly defined to include any type of computer readable storage device and/or storage disk and to exclude propagating signals and transmission media. As used herein, when the phrase "at least" is used as the transition term in a preamble of a claim, it is open-ended in the same manner as the term "comprising" is open ended.

[0074] FIG. 5 is a flow diagram of an example process that may be used to collect media identifiers (e.g., the media ID 122 of FIG. 1) and device and/or user identifiers (e.g., the device/user identifiers 124 of FIGS. 1 and 2) at mobile devices (e.g., the mobile device 106 of FIG. 1). In some examples, instead of or in addition to collecting media identifiers, the example process of FIG. 5 may additionally or alternatively be used to collect search terms (e.g., the search term(s) 1210 of FIG. 12). In the illustrated example, the example process of FIG. 5 is performed at the mobile device 106. However, the example process of FIG. 5 may be performed at any other device.

[0075] Initially, the data collector 112 (FIG. 1) determines whether it should collect data (block 502). For example, the app program 116 (FIG. 1) may trigger the data collector 112 to collect data when the app program 116 presents media (e.g., the media 118 of FIG. 1) or receives one or more search term(s) (e.g., the search term(s) 1210 of FIGS. 12-14). When the data collector 112 determines at block 502 that it should collect data, the data collector 112 retrieves the media ID 122 from the media 118, and/or the search term(s) 1210 (block 504). The data collector 112 also collects one or more of the device/user identifier(s) 124 from the mobile device 106 (block 506). The data collector 112 locates the media ID 122, and/or the search term(s) 1210, and the device/user identifier(s) 124 in a collected data message (e.g., the collected data 126 of FIG. 1 and/or the collected data 1214 of FIG. 12) (block 508). The data collector 112 sends the media ID 122, and/or the search term(s) 1210, and the device/user identifier(s) 124 to a collection entity (block 510). For example, the data collector 112 sends the media ID 122, and/or the search term(s) 1210, and the device/user identifier(s) 124 as the collected data 126 (FIG. 1) and/or 1214 (FIG. 12) to the apps publisher 110 of FIG. 1. The example process of FIG. 5 then ends.

[0076] In some examples in which the encryptor 202 of FIG. 2 is provided in the data collector 112, the encryptor 202 encrypts the device/user identifier(s) 124 at block 508 to generate one or more of the encrypted device/user identifier(s) 208a-i of FIG. 2. In such some examples, the data collector 112 locates the encrypted device/user identifier(s) 208a-i and the media ID 122, and/or the search term(s) 1210, in the collected data 126 and/or 1214 at block 508. In some examples in which the encoder 204 is also provided in the data collector 112, the encoder 204 generates the ACR ID 128 of FIGS. 1-4 by encoding the encrypted device/user identifier(s) 208a-i into the ACR ID 128 at block 508. In such some examples, the data collector 112 locates the ACR ID 128 and the media ID 122, and/or the search term(s) 1210, in the collected data 126 and/or 1214 at block 508. An example process that may be used to encrypt the device/user identifier(s) 124 and encode the encrypted device/user identifiers 208a-i is described below in connection with FIG. 6.

[0077] FIG. 11 is a flow diagram of an example process that may be used to collect media identifiers (e.g., the media ID 122 of FIGS. 1, 9, and 10) and device and/or user identifiers (e.g., the device/user identifier(s) 124 of FIGS. 1, 9, and 10) at a media publisher (e.g., the media publisher 120 of FIGS. 1, 9, and 10). In the illustrated example, the example process of FIG. 11 is performed by a processor system (e.g., a server) at the media publisher 120 in connection with the example system 900 of FIG. 9 and/or the example system 1000 of FIG. 10. However, the example process of FIG. 11 may be performed by any other device.

[0078] Initially, the media publisher 120 receives the device/user identifier(s) 124 (block 1102) from, for example, the data collector 912 of FIG. 9 or the data collector 1012 of FIG. 10. For example, the media publisher 120 may receive the device/user identifier(s) 124 in an HTTP header of an HTTP request from the mobile device 106. The media publisher 120 determines whether it should serve media (e.g., the media 118 of FIGS. 9 and 10) (block 1104) to, for example, the mobile device 106. For example, the media publisher 120 may receive a media serve request from the mobile device 106 that was generated by the app program 116 when executing on the mobile device 106. In the illustrated example, the media serve request is a request to serve an advertisement or other media to the mobile device 106 for presenting while the app program 116 is executing. In some examples, the media serve request is received at block 1102 when the media publisher 120 receives the device/user identifier(s) 124. For example, media publisher 120 may receive the media serve

request from the mobile device 106 in the HTTP request that includes the device/user identifier(s) 124 in its HTTP header.

[0079] When the media publisher 120 determines at block 1104 that it should serve media (e.g., the media 118), the media publisher 120 retrieves the media ID 122 from the media 118 to be served (block 1106). The media publisher 120 serves the media 118 (block 1108). For example, the media publisher 120 may use one or more of the device/user identifier(s) 124 received at block 1102 to identify the mobile device 106 as a receiving device of the served media 118. The media publisher 120 locates the media ID 122 and the device/user identifier(s) 124 in a message (block 1110). For example, in the example system 900 of FIG. 9, the media publisher 120 locates the media ID 122 and the device/user identifier(s) 124 in the collected data message 902. Alternatively, in the example system 1000 of FIG. 10 in which the apparatus 200 of FIG. 2 is implemented at the media publisher 120, the media publisher 120 generates the ACR ID 128 (FIGS. 10 and 2) based on the device/user identifier(s) 124, and locates the media ID 122 and the ACR ID 128 in the impression data 130 at block 1110. The media publisher 120 sends the media ID 122 and the device/user identifier(s) 124 (block 1112), for example, as the collected data 902 to the app publisher 110 as shown in FIG. 9, or as the impression data 130 to the AME 108 as shown in FIG. 10. The example process of FIG. 11 then ends.

[0080] FIG. 15 is a flow diagram of an example process that may be executed to collect search terms (e.g., the search term(s) 1210 of FIGS. 12-14) and device and/or user identifiers (e.g., the device/user identifiers 124 of FIGS. 12-14) at a search provider (e.g., the search provider 1212 of FIGS. 12-14). In the illustrated example, the example process of FIG. 15 is performed by a processor system (e.g., a server) at the search provider 1212 in connection with the example system 1300 of FIG. 13 and/or the example system 1400 of FIG. 14. However, the example process of FIG. 15 may be performed by any other device.

[0081] Initially, the search provider 1212 receives the device/user identifier(s) 124 (block 1502) from, for example, the data collector 1312 of FIG. 13 or the data collector 1412 of FIG. 14. For example, the search provider 1212 may receive the device/user identifier(s) 124 in an HTTP header of an HTTP request from the mobile device 106. The search provider 1212 receives the search term (s) 1210 from the app program 1204 (block 1504). The search provider 1212 serves search results 1506 (block 1506). For example, the search provider 1212 may use one or more of the

device/user identifier(s) 124 received at block 1502 to identify the mobile device 106 as a receiving device of the search results. The search provider 1212 locates the search term(s) 1210 and the device/user identifier(s) 124 in a message (block 1508). For example, in the example system 1300 of FIG. 13, the search provider 1212 locates the search term(s) 1210 and the device/user identifier(s) 124 in the collected data message 1302. Alternatively, in the example system 1400 of FIG. 14 in which the apparatus 200 of FIG. 2 is implemented at the search provider 1212, the search provider 1212 generates the ACR ID 128 (FIGS. 14 and 2) based on the device/user identifier(s) 124, and locates the search term(s) 1210 and the ACR ID 128 in the user-interest data 1216 at block 1508. The search provider 1212 sends the search term(s) 1210 and the device/user identifier(s) 124 (block 1510), for example, as the collected data 1302 to the app publisher 110 as shown in FIG. 13, or as the user-interest data 1216 to the AME 108 as shown in FIG. 14. The example process of FIG. 15 then ends.

[0082] FIG. 6 is a flow diagram of an example process to encrypt device and/or user identifiers (e.g., the device/user identifier(s) 124 of FIGS. 1 and 2), and to encode encrypted device and/or user identifiers (e.g., the encrypted device/user identifier(s) 208a-i of FIGS. 2-4) into the ACR ID 128 of FIGS. 1-4. The example process of FIG. 6 may be performed wholly or partially at the app publisher 110 of FIGS. 1, 9, and 10 (or another collection entity), wholly or partially at the mobile device 106 (e.g., at block 508 of the example process of FIG. 5), wholly or partially at the media publisher 120 of FIGS. 1, 9, and 10, and/or wholly or partially at the search provider 1212 of FIGS. 12-14. In some examples, operations performed by the encryptor 202 (FIG. 2) may be performed at the mobile device 106, and operations performed by the encoder 204 (FIG. 2) may be performed at the app publisher 110, at the media publisher 120, and/or at the search provider 1212.

[0083] Initially, the encryptor 202 (FIG. 2) receives one or more of the device/user identifier(s) 124 (FIGS. 1 and 2) (block 602). The encryptor 202 encrypts the device/user identifier(s) 124 (block 604) to generate the encrypted device/user identifier(s) 208a-i (FIG. 2). In the illustrated example, the encryptor 202 provides corresponding partner database proprietor identifiers to corresponding ones of the encrypted device/user identifier(s) 208a-i (block 606), for example, by appending, prepending, concatenating, or otherwise associating the partner database proprietor identifiers to or with the encrypted device/user identifier(s) 208a-i so that the partner

database proprietor identifiers are accessible to the AME 108 without decrypting the encrypted device/user identifier(s) 208a-i. The encoder 204 (FIG. 2) encodes the encrypted device/user identifier(s) 208a-i into the ACR ID 128 (block 608). In the illustrated example, the encoder 204 associates the ACR ID 128 with the corresponding media ID 122, and/or the search term(s) 1210 (block 610). The encoder 204 sends the ACR ID 128 and the media ID 122, and/or the search term(s) 1210, to the AME 108 (block 612), for example, in the impression data 130 (FIGS. 1, 9, and 10). In some examples, the media ID 112 and/or the search term(s) 1210 are encrypted prior to transmission. The example process of FIG. 6 then ends.

[0084] FIG. 7 is a flow diagram of an example process that may be used to decode encrypted device and/or user identifiers (e.g., the encrypted device/user identifiers 208a-i of FIGS. 2-4) from the ACR ID 128 of FIGS. 1-4, and collect user information associated with the encrypted device and/or user identifiers from one or more corresponding partner database proprietor(s) (e.g., one or more of the partner database proprietors 102a-e of FIGS. 1, 3, and 4). The example process of FIG. 7 may be performed at the AME 108 (FIG. 1), for example, by the server 132 (FIG. 1).

[0085] Initially, the server 132 receives the ACR ID 128 and the associated media ID 122, and/or the search term(s) 1210 (block 702). For example, the server 132 may receive the ACR ID 128 and the media ID 122 in the impression data 130 from the app publisher 110, from the media publisher 120, and/or from the mobile device 106 of FIGS. 1, 9, and 10. Additionally or alternatively, the server 132 may receive the ACR ID 128 and the search term(s) 1210 in the user-interest data 1216 from the app publisher 110, from the search provider 1212, and/or from the mobile device 106 of FIGS. 12-14. The decoder 302 (FIGS. 3 and 4) decodes one or more of the encrypted device/user identifier(s) 208a-i from the ACR ID 128 (block 704). The decoder 302 sends corresponding ones of the encrypted device/user identifier(s) 208a-i to corresponding ones of the partner database proprietor(s) 102a-e (block 706), for example, based on partner database proprietor identifiers provided to or associated with the encrypted device/user identifiers 208a-i by the encryptor 202 of FIG. 2 at block 606 of FIG. 6. The server 132 receives one or more of the user information 102a-e from one or more of the partner database proprietor(s) 102a-e (block 708). The server 132 logs a media impression for the media ID 122 (block 710). In addition, the server 132 associates the user information from at least one of the one or more user information 102a-e with the logged impression for the media ID

122, and/or with the search term(s) 1210 (block 712). The example process of FIG. 7 then ends.

[0086] FIG. 8 is a block diagram of an example computer 800 capable of executing the instructions of FIGS. 5-7, 11, and 15. The computer 800 can be, for example, a server, a personal computer, or any other type of computing device. The system 800 of the illustrated example includes a processor 812. For example, the processor 812 can be implemented by one or more microprocessors or controllers from any desired family or manufacturer.

[0087] The processor 812 includes a local memory 813 (e.g., a cache) and is in communication with a main memory including a volatile memory 814 and a non-volatile memory 816 via a bus 818. The volatile memory 814 may be implemented by Synchronous Dynamic Random Access Memory (SDRAM), Dynamic Random Access Memory (DRAM), RAMBUS Dynamic Random Access Memory (RDRAM) and/or any other type of random access memory device. The non-volatile memory 816 may be implemented by flash memory and/or any other desired type of memory device. Access to the main memory 814, 816 is controlled by a memory controller.

[0088] The computer 800 also includes an interface circuit 820. The interface circuit 820 may be implemented by any type of interface standard, such as an Ethernet interface, a universal serial bus (USB), and/or a PCI express interface.

[0089] One or more input devices 822 are connected to the interface circuit 820. The input device(s) 822 permit a user to enter data and commands into the processor 812. The input device(s) can be implemented by, for example, a keyboard, a mouse, a touchscreen, a track-pad, a trackball, isopoint and/or a voice recognition system.

[0090] One or more output devices 824 are also connected to the interface circuit 820. The output devices 824 can be implemented, for example, by display devices (e.g., a liquid crystal display, a cathode ray tube display (CRT), a printer and/or speakers). The interface circuit 820, thus, typically includes a graphics driver card.

[0091] The interface circuit 820 also includes a communication device such as a modem or network interface card to facilitate exchange of data with external computers via a network 826 (e.g., an Ethernet connection, a digital subscriber line (DSL), a telephone line, coaxial cable, a cellular telephone system, etc.).

[0092] The computer 800 also includes one or more mass storage devices 828 for storing software and data. Examples of such mass storage devices 828 include

floppy disk drives, hard drive disks, compact disk drives and digital versatile disk (DVD) drives.

[0093] Coded instructions 832 representative of machine readable instructions of FIGS. 5-7, 11, and 15 may be stored in the mass storage device 828, in the volatile memory 814, in the non-volatile memory 816, and/or on a removable storage medium such as a CD or DVD.

[0094] Although certain example methods, apparatus and articles of manufacture have been disclosed herein, the scope of coverage of this patent is not limited thereto. On the contrary, this patent covers all methods, apparatus and articles of manufacture fairly falling within the scope of the claims of this patent.

CLAIMS

1. A method to monitor usage of a device, the method comprising:

installing an application having a data collector on the device;

collecting, via the data collector, a media identifier indicative of media presented at the device, the collecting performed by the data collector based on the application that does not employ cookies in the device;

encrypting a user identifier that identifies the user of the device, the encrypting of the user identifier based on a first encryption key corresponding to a first database proprietor;

encrypting a device identifier that identifies the device, the encrypting of the device identifier based on a second encryption key corresponding to a second database proprietor; and

sending encrypted user identifier, the encrypted device identifier, and the media identifier to a data collection server.

2. A method as defined in claim 1, further including encoding the encrypted user identifier and the encrypted device identifier in a single identifier, wherein sending the encrypted user identifier and the encrypted device identifier to the data collection server includes sending the single identifier to the data collection server.

3. A method as defined in claim 1, further including associating a first database proprietor identifier with the encrypted user identifier, and associating a second database proprietor identifier with the encrypted device identifier, the first database proprietor identifier indicative of the encrypted user identifier corresponding to the first database proprietor, and the second database proprietor identifier indicative of the encrypted device identifier corresponding to the second database proprietor.

4. A method as defined in claim 1, wherein the first database proprietor is a social network service, and the second database proprietor is a wireless service provider.

Date Reçue/Date Received 2021-07-27

5. A method as defined in claim 1, wherein the first and second user information include demographic information collected from the user of the device by the first and second database proprietors.

6. An apparatus to track usage of a device, the apparatus comprising:

a memory; and

a processor to install an application including a data collector in the memory, the processor to execute the data collector to:

collect a search term indicative of a search requested via the device, the collecting performed by the processor based on the application that does not employ cookies in the device;

encrypt a user identifier that identifies the user of the device, the encrypting of the user identifier based on a first encryption key corresponding to a first database proprietor;

encrypt a device identifier that identifies the device, the encrypting of the device identifier based on a second encryption key corresponding to a second database proprietor; and

send the encrypted user identifier, the encrypted device identifier, and the search term to a data collection server.

7 An apparatus as defined in claim 6, wherein the search term is encrypted.

8. An apparatus as defined in claim 6, wherein the data collector is to encode the encrypted user identifier and the encrypted device identifier in a single identifier, and wherein the data collector is to send the encrypted user identifier and the encrypted device identifier to the data collection server by sending the single identifier to the data collection server.

9. An apparatus as defined in claim 8, wherein the data collector is to encode the search term as part of the single identifier.

10. An apparatus as defined in claim 6, wherein the data collector is to associate a first database proprietor identifier with the encrypted user identifier, and to associate a second

Date Reçue/Date Received 2021-07-27

database proprietor identifier with the encrypted device identifier, the first database proprietor identifier indicative of the encrypted user identifier corresponding to the first database proprietor, and the second database proprietor identifier indicative of the encrypted device identifier corresponding to the second database proprietor.

11. An apparatus as defined in claim 6, wherein the first database proprietor is a social network service, and the second database proprietor is a wireless service provider.

12. An apparatus as defined in claim 6, wherein the search term is a term entered at the device to at least one of search information on the Internet, search for a product, search for a website, and search in a website.

13. A machine accessible storage medium storing computer-readable instructions that, when executed, cause a processor to at least:

install an application having a data collector on a device;

collect, via the data collector, a search term, the search term indicative of a search requested via the device, the collecting performed based on the application that does not employ cookies in the device;

encrypt a user identifier that identifies the user of the device, the encrypting of the user identifier based on a first encryption key corresponding to a first database proprietor;

encrypt a device identifier that identifies the device, the encrypting of the device identifier based on a second encryption key corresponding to a second database proprietor; and

send the encrypted user identifier, the encrypted device identifier, and the search term to a data collection server.

14. A machine accessible storage medium as defined in claim 13, wherein the processor is a server separate from the device and in communication with the device.

15. A machine accessible storage medium as defined in claim 13, wherein the instructions cause the processor to associate a first database proprietor identifier with the encrypted user

Date Reçue/Date Received 2021-07-27

identifier, and to associate a second database proprietor identifier with the encrypted device identifier.

16. A machine accessible storage medium as defined in claim 13, wherein the first database proprietor is a social network service, and the second database proprietor is a wireless service provider.

17. A machine accessible storage medium as defined in claim 13, wherein the search term is a term entered at the device to at least one of search information on the Internet, search for a product, search a website, and search for in a website.

18. A method as defined in claim 1, further including installing an application having a data collector on the device, wherein the collecting of the media identifier is performed using the data collector.

19. A method as defined in claim 1, wherein the first database proprietor stores first user information associated with the user identifier, and the second database proprietor stores second user information associated with the device identifier.

20. An apparatus as defined in claim 6, wherein the first database proprietor stores first user information associated with the user identifier, and the second database proprietor stores second user information associated with the device identifier.

21. A machine accessible storage medium as defined in claim 13, wherein the instructions cause the processor to encrypt the search term before sending the search term to the data collection server.

22. A machine accessible storage medium as defined in claim 13, wherein the instructions cause the processor to encode the encrypted user identifier and the encrypted device identifier in a single identifier, and to send the encrypted user identifier and the encrypted device identifier to the data collection server by sending the single identifier to the data collection server.

Date Reçue/Date Received 2021-07-27

23. A machine accessible storage medium as defined in claim 22, wherein the instructions cause the processor to encode the search term as part of the single identifier.

24. A machine accessible storage medium as defined in claim 15, wherein the first database proprietor identifier is indicative of the encrypted user identifier corresponding to the first database proprietor, and the second database proprietor identifier is indicative of the encrypted device identifier corresponding to the second database proprietor.

25. A machine accessible storage medium as defined in claim 13, wherein the first database proprietor is a social network service, and the second database proprietor is a wireless service provider.

26. A method of any one of claims 1 to 5, 18 and 19, wherein the device is a mobile device.

27. An apparatus of any one of claims 6 to 12 and 20, wherein the device is a mobile device.

28. A machine accessible storage medium of any one of claims 13 to 17 and 21 to 25, wherein the device is a mobile device.

29. A machine accessible storage medium storing computer-readable instructions that, when executed, cause a processor to at least:

install an application having a data collector on a device;

collect, via the data collector, a media identifier indicative of media presented at the device, the collecting performed based on the application that does not employ cookies in the device;

encrypt a user identifier that identifies the user of the device, the encrypting of the user identifier based on a first encryption key corresponding to a first database proprietor having first user information associated with the user identifier;

Date Reçue/Date Received 2021-07-27

encrypt a device identifier that identifies the device, the encrypting of the device identifier based on a second encryption key corresponding to a second database proprietor having second user information associated with the device identifier; and

send the encrypted user identifier, the encrypted device identifier, and the media identifier to a data collection server.

30. A machine accessible storage medium as defined in claim 29, wherein the instructions cause the processor to encode the encrypted user identifier and the encrypted device identifier in a single identifier, wherein to send the encrypted user identifier and the encrypted device identifier to the data collection server includes sending the single identifier to the data collection server.

31. A machine accessible storage medium as defined in claim 29, wherein the instructions cause the processor to associate a first database proprietor identifier with the encrypted user identifier, and to associate a second database proprietor identifier with the encrypted device identifier, the first database proprietor identifier indicative of the encrypted user identifier corresponding to the first database proprietor, and the second database proprietor identifier indicative of the encrypted device identifier corresponding to the second database proprietor.

32. A machine accessible storage medium as defined in claim 29, wherein the first database proprietor is a social network service, and the second database proprietor is a wireless service provider.

33. A machine accessible storage medium as defined in claim 29, wherein the first and second user information include demographic information collected from the user of the device by the first and second database proprietors.

34. A machine accessible storage medium of any one of claims 29 to 33, wherein the device is a mobile device.

35. A method comprising:

Date Reçue/Date Received 2021-07-27

installing an application having a data collector on a mobile device;

collecting, via the data collector, a search term indicative of a search requested via the device, the collecting performed by the data collector based on the application that does not employ cookies in the device;

encrypting a user identifier that identifies the user of the device, the encrypting of the user identifier based on a first encryption key corresponding to a first database proprietor;

encrypting a device identifier that identifies the device, the encrypting of the device identifier based on a second encryption key corresponding to a second database proprietor; and

sending the encrypted user identifier, the encrypted device identifier, and the search term to a data collection server.

36. A method as defined in claim 35, further including associating a first database proprietor identifier with the encrypted user identifier, and associating a second database proprietor identifier with the encrypted device identifier.

37. A method as defined in claim 35, wherein the first database proprietor is a social network service, and the second database proprietor is a wireless service provider.

38. A method as defined in claim 35, wherein the search term is a term entered at the device to at least one of search information on the Internet, search for a product, search a website, and search for in a website.

39. A method as defined in claim 35, further including encrypting the search term before sending the search term to the data collection server.

40. A method as defined in claim 35, further including encoding the encrypted user identifier and the encrypted device identifier in a single identifier, and to send the encrypted user identifier and the encrypted device identifier to the data collection server by sending the single identifier to the data collection server.

Date Reçue/Date Received 2021-07-27

41. A method as defined in claim 38, further including associating the single identifier with the search term.

42. A method as defined in claim 36, wherein the first database proprietor identifier is indicative of the encrypted user identifier corresponding to the first database proprietor, and the second database proprietor identifier is indicative of the encrypted device identifier corresponding to the second database proprietor.

43. A method as defined in claim 35, wherein the first database proprietor is a social network service, and the second database proprietor is a wireless service provider.

44. A method of any one of claims 35 to 43, wherein the device is a mobile device.

45. An apparatus comprising:

a data collector to be provided with an application to be installed in a device, the data collector to collect a user identifier and a device identifier based on the application that does not employ cookies in the device;

an encryptor to:

encrypt the user identifier that identifies a user of the device, the encrypting of the user identifier based on a first encryption key corresponding to a first database proprietor; and

encrypt the device identifier that identifies the device, the encrypting of the device identifier based on a second encryption key corresponding to a second database proprietor; and

a processor to install the application including the data collector in the device, the processor to:

send the encrypted user identifier, the encrypted device identifier, and a media identifier to a data collection server, the media identifier indicative of media presented at the device.

Date Reçue/Date Received 2021-07-27

46. An apparatus as defined in claim 45, wherein the encryptor and the processor are located in a server that is separate from the device and in communication with the device.

47. An apparatus as defined in claim 45, wherein the encryptor is to associate a first database proprietor identifier with the encrypted user identifier, and to associate a second database proprietor identifier with the encrypted device identifier, the first database proprietor identifier indicative of the encrypted user identifier corresponding to the first database proprietor, and the second database proprietor identifier indicative of the encrypted device identifier corresponding to the second database proprietor.

48. An apparatus as defined in claim 45, wherein the first database proprietor is a social network service, and the second database proprietor is a wireless service provider.

49. An apparatus as defined in claim 45, wherein the media is an advertisement.

50. An apparatus as defined in claim 45, further including an encoder to encode the encrypted user identifier and the encrypted device identifier in a single identifier, and to send the encrypted user identifier and the encrypted device identifier to the data collection server by sending the single identifier to the data collection server.

51. An apparatus as defined in claim 50, wherein the encoder is to associate the single identifier with the media identifier.

52. An apparatus as defined in claim 46, wherein the first database proprietor stores first user information associated with the user identifier, and the second database proprietor stores second user information associated with the device identifier.

53. An apparatus as defined in claim 46, wherein the first and second user information include demographic information collected from the user of the device by the first and second database proprietors.

Date Reçue/Date Received 2021-07-27

54. An apparatus of any one of claims 45 to 53, wherein the device is a mobile device.

55. A method comprising:

obtaining a plurality of first identifiers and a media identifier collected by a data collector installed at a device in connection with an application, the first identifiers identifying at least one of the device and a user of the device, and the media identifier indicative of media presented via the application at the device;

generating a plurality of encrypted identifiers by encrypting the first identifiers, respective ones of the encrypted identifiers decodable by corresponding database proprietors to which the respective encrypted identifiers pertain; and

sending the plurality of encrypted identifiers in association with the media identifier to an audience measurement entity.

56. A method as defined in claim 55, wherein the plurality of the encrypted identifiers are generated using respective encryption keys corresponding to respective ones of the database proprietors.

57. A method as defined in claim 55, wherein the first identifiers include at least one of an international mobile equipment identity (IMEI), a mobile equipment identifier (MEID), a media access control (MAC) address, an app store identifier, an open source unique device identifier (OpenUDID), an open device identification number (ODIN), a login identifier, an email address, user agent data, and a third-party service identifier.

58. A method as defined in claim 55, wherein the respective ones of the first identifiers correspond to respective second identifiers stored by corresponding ones of the database proprietors in association with user information corresponding to the user of the device.

59. A method as defined in claim 55, wherein the database proprietors include at least one of a wireless service carrier, a mobile software provider, a mobile service provider, a social network service provider, and an online retailer.

Date Reçue/Date Received 2021-07-27

60. A method as defined in claim 55, further including sending the plurality of the encrypted identifiers to the audience measurement entity as a single identifier including the plurality of the encrypted identifiers.

61. A method as defined in claim 55, further including sending the data collector to the device in association with the application for installation at the device.

62. A method as defined in claim 55, wherein the obtaining of the plurality of first identifiers, the generating of the plurality of the encrypted identifiers, and the sending of the plurality of the encrypted identifiers are performed by an application publisher.

63. A method as defined in claim 55, wherein the obtaining of the plurality of first identifiers, the generating of the plurality of the encrypted identifiers, and the sending of the plurality of the encrypted identifiers are performed by a media publisher.

64. A method of any one of claims 55 to 63, wherein the device is a mobile device.

65. An apparatus comprising:

an encryptor executed by a processor to generate a plurality of encrypted identifiers by encrypting first identifiers collected by a data collector installed at a device in connection with an application, the first identifiers identifying at least one of the device and a user of the device, and respective ones of the encrypted identifiers decodable by corresponding database proprietors to which the respective encrypted identifiers pertain; and

a communication interface to send to an audience measurement entity the encrypted identifiers in association with a media identifier, the media identifier collected by the data collector at the device, the media identifier indicative of media presented via the application at the device.

66. An apparatus as defined in claim 65, wherein the encryptor is to generate the plurality of the encrypted identifiers using respective encryption keys corresponding to respective ones of the database proprietors.

Date Reçue/Date Received 2021-07-27

67. An apparatus as defined in claim 65, wherein the first identifiers include at least one of an international mobile equipment identity (IMEI), a mobile equipment identifier (MEID), a media access control (MAC) address, an app store identifier, an open source unique device identifier (OpenUDID), an open device identification number (ODIN), a login identifier, an email address, user agent data, and a third-party service identifier.

68. An apparatus as defined in claim 65, wherein the respective ones of the first identifiers correspond to second identifiers stored by corresponding ones of the database proprietors in association with user information corresponding to the user of the device.

69. An apparatus as defined in claim 65, wherein the database proprietors include at least one of a wireless service carrier, a mobile software provider, a mobile service provider, a social network service provider, and an online retailer.

70. An apparatus as defined in claim 65, further including an encoder to encode the encrypted identifiers into a single identifier including the encrypted identifiers, and the communication interface is to send the encrypted identifiers as the single identifier to the audience measurement entity.

71. An apparatus as defined in claim 65, further including sending the data collector to the device in association with the application for installation at the device.

72. An apparatus as defined in claim 65, wherein the encryptor, the processor, and the communication interface are to be operated at an application publisher location.

73. An apparatus as defined in claim 65, wherein the encryptor, the processor, and the communication interface are to be operated at a media publisher location.

74. An apparatus of any one of claims 65 to 73, wherein the device is a mobile device.

Date Reçue/Date Received 2021-07-27

75. A machine accessible storage medium storing computer-readable instructions that, when executed, cause a machine to at least:

obtain a plurality of first identifiers and a media identifier collected by a data collector installed at a device in connection with an application, the first identifiers identifying at least one of the device and a user of the device, and the media identifier indicative of media presented via the application at the device;

generate a plurality of encrypted identifiers by encrypting the first identifiers, respective ones of the encrypted identifiers decodable by corresponding database proprietors to which the respective encrypted identifiers pertain; and

send the plurality of encrypted identifiers in association with the media identifier to an audience measurement entity.

76. A machine accessible storage medium as defined in claim 75, wherein the instructions cause the machine to generate the plurality of the encrypted identifiers using respective encryption keys corresponding to respective ones of the database proprietors.

77. A machine accessible storage medium as defined in claim 75, wherein the first identifiers include at least one of an international mobile equipment identity (IMEI), a mobile equipment identifier (MEID), a media access control (MAC) address, an app store identifier, an open source unique device identifier (OpenUDID), an open device identification number (ODIN), a login identifier, an email address, user agent data, and a third-party service identifier.

78. A machine accessible storage medium as defined in claim 75, wherein the respective ones of the first identifiers correspond to second identifiers stored by corresponding ones of the database proprietors in association with user information corresponding to the user of the device.

79. A machine accessible storage medium as defined in claim 75, wherein the database proprietors include at least one of a wireless service carrier, a mobile software provider, a mobile service provider, a social network service provider, and an online retailer.

Date Reçue/Date Received 2021-07-27

80. A machine accessible storage medium as defined in claim 75, wherein the instructions cause the machine to send the encrypted identifiers to the audience measurement entity as a single identifier including the encrypted identifiers.

81. A machine accessible storage medium as defined in claim 75, wherein the instructions cause the machine to send the data collector to the device in association with the application for installation at the device.

82. A machine accessible storage medium as defined in claim 75, wherein the instructions are to be executed by the machine at an application publisher location.

83. A machine accessible storage medium as defined in claim 75, wherein the instructions are to be executed by the machine at a media publisher location.

84. A machine accessible storage medium of any one of claims 75 to 83, wherein the device is a mobile device.

85. A method, comprising:

collecting, by executing an instruction with a processor, first and second identifiers based on use of an application that does not employ cookies, the first identifier identifying at least one of a device and a user of the device to a first database proprietor that stores first user information associated with the first identifier, and the second identifier identifying the at least one of the device and the user of the device to a second database proprietor that stores second user information associated with the second identifier;

encrypting, by executing an instruction with the processor, the first identifier to generate a first encrypted identifier for access by the first database proprietor;

encrypting, by executing an instruction with the processor, the second identifier to generate a second encrypted identifier for access by the second database proprietor; and

sending in a network communication to a data collection server the first and second encrypted identifiers and at least one of a media identifier indicative of media accessed at the device and a search term collected at the device.

Date Reçue/Date Received 2021-07-27

86. The method as defined in claim 85, further including encrypting the first identifier to generate the first encrypted identifier for access by the first database proprietor, encrypting the second identifier to generate the second encrypted identifier for access by the second database proprietor, the sending of the first and second identifiers in the network communication to the data collection server being the sending of the first and second encrypted identifiers to the data collection server.

87. The method as defined in claim 86, wherein the first and second encrypted identifiers are generated using respective encryption keys corresponding to respective ones of the database proprietors.

88. The method as defined in claim 85, wherein the first and second identifiers include at least one of an international mobile equipment identity (IMEI), a mobile equipment identifier (MEID), a media access control (MAC) address, an app store identifier, an open source unique device identifier (OpenUDID), an open device identification number (ODIN), a login identifier, an email address, user agent data, and a third-party service identifier.

89. The method as defined in claim 85, wherein the first and second database proprietors include at least one of a wireless service carrier, a mobile software provider, a mobile service provider, a social network service provider, and an online retailer.

90. The method as defined in claim 85, wherein the first and second identifiers are sent to the data collection server as a single identifier including the first and second identifiers.

91. The method as defined in claim 85, wherein the collecting of the first and second identifiers is performed by a data collector installed in the device in association with the application.

Date Reçue/Date Received 2021-07-27

92. The method as defined in claim 85, wherein the collecting of the first and second identifiers and the sending of the first and second identifiers in the network communication to the data collection server are performed by the device.

93. The method as defined in claim 85, wherein the collecting of the first and second identifiers and the sending of the first and second identifiers in the network communication to the data collection server are performed by an application publisher.

94. The method as defined in claim 85, wherein the collecting of the first and second identifiers and the sending of the first and second identifiers in the network communication to the data collection server are performed by a media publisher.

95. An apparatus, comprising:

a processor to:

collect first and second identifiers based on use of an application that does not employ cookies, the first identifier identifying at least one of a device and a user of the device to a first database proprietor that stores first user information associated with the first identifier, and the second identifier identifying the at least one of the device and the user of the device to a second database proprietor that stores second user information associated with the second identifier; and

encrypt the first identifier to generate a first encrypted identifier for access by the first database proprietor, encrypt the second identifier to generate a second encrypted identifier for access by the second database proprietor; and

an interface circuit to send in a network communication to a data collection server the first and second identifiers and at least one of a media identifier indicative of media accessed at the device and a search term collected at the device.

96. The apparatus as defined in claim 95, further including an encryptor to:

encrypt the first identifier to generate a first encrypted identifier for access by the first database proprietor;

Date Reçue/Date Received 2021-07-27

encrypt the second identifier to generate a second encrypted identifier for access by the second database proprietor, the sending of the first and second identifiers in the network communication to the data collection server being the sending of the first and second encrypted identifiers to the data collection server.

97. The apparatus as defined in claim 96, wherein the encryptor is to generate the first and second encrypted identifiers using respective encryption keys corresponding to respective ones of the database proprietors.

98. The apparatus as defined in claim 95, wherein the first and second identifiers include at least one of an international mobile equipment identity (IMEI), a mobile equipment identifier (MEID), a media access control (MAC) address, an app store identifier, an open source unique device identifier (OpenUDID), an open device identification number (ODIN), a login identifier, an email address, user agent data, and a third-party service identifier.

99. The apparatus as defined in claim 95, wherein the first and second database proprietors include at least one of a wireless service carrier, a mobile software provider, a mobile service provider, a social network service provider, and an online retailer.

100. The apparatus as defined in claim 95, wherein the interface circuit is to send the first and second identifiers to the data collection server as a single identifier including the first and second identifiers.

101. The apparatus as defined in claim 95, wherein the interface circuit is to send a data collector to the device in association with the application for installation at the device.

102. The apparatus as defined in claim 95, wherein the processor and the interface circuit are located in the device.

103. The apparatus as defined in claim 95, wherein the processor and the interface circuit are located in an application publisher.

Date Reçue/Date Received 2021-07-27

104. The apparatus as defined in claim 95, wherein the processor, the encryptor, and the interface circuit are located in a media publisher.

105. A tangible computer readable storage medium comprising instructions that, when executed, cause a processor to at least:

collect first and second identifiers based on use of an application that does not employ cookies, the first identifier identifying at least one of a device and a user of the device to a first database proprietor that stores first user information associated with the first identifier, and the second identifier identifying the at least one of the device and the user of the device to a second database proprietor that stores second user information associated with the second identifier;

encrypt the first identifier to generate a first encrypted identifier for access by the first database proprietor, encrypt the second identifier to generate a second encrypted identifier for access by the second database proprietor; and

send in a network communication to a data collection server the first and second identifiers and at least one of a media identifier indicative of media accessed at the device and a search term collected at the device.

106. The tangible computer readable storage medium as defined in claim 105, wherein the instructions are to further cause the processor to:

encrypt the first identifier to generate a first encrypted identifier for access by the first database proprietor; and

encrypt the second identifier to generate a second encrypted identifier for access by the second database proprietor, the sending of the first and second identifiers in the network communication to the data collection server being the sending of the first and second encrypted identifiers to the data collection server.

107. The tangible computer readable storage medium as defined in claim 106, wherein the instructions are to further cause the processor to generate the first and second encrypted identifiers using respective encryption keys corresponding to respective ones of the database proprietors.

Date Reçue/Date Received 2021-07-27

108. The tangible computer readable storage medium as defined in claim 105, wherein the first and second identifiers include at least one of an international mobile equipment identity (IMEI), a mobile equipment identifier (MEID), a media access control (MAC) address, an app store identifier, an open source unique device identifier (OpenUDID), an open device identification number (ODIN), a login identifier, an email address, user agent data, and a third-party service identifier.

109. The tangible computer readable storage medium as defined in claim 105, wherein the first and second database proprietors include at least one of a wireless service carrier, a mobile software provider, a mobile service provider, a social network service provider, and an online retailer.

110. The tangible computer readable storage medium as defined in claim 105, wherein the instructions cause the processor to send the first and second identifiers to the data collection server as a single identifier including the first and second identifiers.

111. The tangible computer readable storage medium as defined in claim 105, wherein the instructions cause the processor to execute a data collector to perform the collecting of the first and second identifiers, the data collector installed in the device in association with the application.

112. The tangible computer readable storage medium as defined in claim 105, wherein the processor is located in the device.

113. The tangible computer readable storage medium as defined in claim 105, wherein the processor is located in an application publisher.

114. The tangible computer readable storage medium as defined in claim 105, wherein the processor is located in a media publisher.

Date Reçue/Date Received 2021-07-27

115. An apparatus, comprising:

at least one memory;

instructions in the apparatus; and

processor circuitry to execute the instructions to at least:

collect first and second identifiers based on use of an application that does not employ cookies, the first identifier identifying at least one of a device and a user of the device to a first database proprietor that stores first user information associated with the first identifier, and the second identifier identifying the at least one of the device and the user of the device to a second database proprietor that stores second user information associated with the second identifier;

encrypt the first identifier to generate a first encrypted identifier for access by the first database proprietor;

encrypt the second identifier to generate a second encrypted identifier for access by the second database proprietor; and

send in a network communication to a data collection server the first and second encrypted identifiers and at least one of a media identifier indicative of media accessed at the device and a search term collected at the device.

116. The apparatus as defined in claim 115, wherein the processor circuitry is to execute the instructions to encrypt the first identifier to generate the first encrypted identifier for access by the first database proprietor, encrypting the second identifier to generate the second encrypted identifier for access by the second database proprietor, the sending of the first and second identifiers in the network communication to the data collection server being the sending of the first and second encrypted identifiers to the data collection server.

117. The apparatus as defined in claim 116, wherein the processor circuitry is to execute the instructions to encrypt the first and second identifiers using respective encryption keys corresponding to respective ones of the database proprietors.

118. The apparatus as defined in claim 115, wherein the first and second identifiers include at least one of an international mobile equipment identity (IMEI), a mobile equipment identifier

Date Reçue/Date Received 2021-07-27

(MEID), a media access control (MAC) address, an app store identifier, an open source unique device identifier (OpenUDID), an open device identification number (ODIN), a login identifier, an email address, user agent data, and a third-party service identifier.

119. The apparatus as defined in claim 115, wherein the first and second database proprietors include at least one of a wireless service carrier, a mobile software provider, a mobile service provider, a social network service provider, and an online retailer.

120. The apparatus as defined in claim 115, wherein the processor circuitry is to execute the instructions to send the first and second identifiers to the data collection server as a single identifier including the first and second identifiers.

121. The apparatus as defined in claim 115, wherein the collecting of the first and second identifiers is performed by a data collector installed in the device in association with the application.

122. The apparatus as defined in claim 115, wherein the collecting of the first and second identifiers and the sending of the first and second identifiers in the network communication to the data collection server are performed by the device.

123. The apparatus as defined in claim 115, wherein the collecting of the first and second identifiers and the sending of the first and second identifiers in the network communication to the data collection server are performed by an application publisher.

124. The apparatus as defined in claim 115, wherein the collecting of the first and second identifiers and the sending of the first and second identifiers in the network communication to the data collection server are performed by a media publisher.

125. The apparatus as defined in claim 115, wherein the processor circuitry is located in a media publisher.

Date Reçue/Date Received 2021-07-27

126. An apparatus, comprising:

means for processing to:

collect first and second identifiers based on use of an application that does not employ cookies, the first identifier identifying at least one of a device and a user of the device to a first database proprietor that stores first user information associated with the first identifier, and the second identifier identifying the at least one of the device and the user of the device to a second database proprietor that stores second user information associated with the second identifier;

encrypt the first identifier to generate a first encrypted identifier for access by the first database proprietor; and

encrypt the second identifier to generate a second encrypted identifier for access by the second database proprietor; and

means for communicating to send in a network communication to a data collection server the first and second identifiers and at least one of a media identifier indicative of media accessed at the device and a search term collected at the device.

127. The apparatus as defined in claim 126, further including means for encrypting to:

encrypt the first identifier to generate the first encrypted identifier for access by the first database proprietor; and

encrypt the second identifier to generate the second encrypted identifier for access by the second database proprietor, the sending of the first and second identifiers in the network communication to the data collection server being the sending of the first and second encrypted identifiers to the data collection server.

128. The apparatus as defined in claim 127, wherein the means for encrypting is to generate the first and second encrypted identifiers using respective encryption keys corresponding to respective ones of the database proprietors.

129. The apparatus as defined in claim 126, wherein the first and second identifiers include at least one of an international mobile equipment identity (IMEI), a mobile equipment identifier (MEID), a media access control (MAC) address, an app store identifier, an open source unique

Date Reçue/Date Received 2021-07-27

device identifier (OpenUDID), an open device identification number (ODIN), a login identifier, an email address, user agent data, and a third-party service identifier.

130. The apparatus as defined in claim 126, wherein the first and second database proprietors include at least one of a wireless service carrier, a mobile software provider, a mobile service provider, a social network service provider, and an online retailer.

131. The apparatus as defined in claim 126, wherein the means for communicating is to send the first and second identifiers to the data collection server as a single identifier including the first and second identifiers.

132. The apparatus as defined in claim 126, wherein the means for communicating is to send the data collector to the device in association with the application for installation at the device.

133. The apparatus as defined in claim 126, wherein the means for processing and the means for communicating are located in the device.

134. The apparatus as defined in claim 126, wherein the means for processing and the means for communicating are located in an application publisher.

Date Reçue/Date Received 2021-07-27

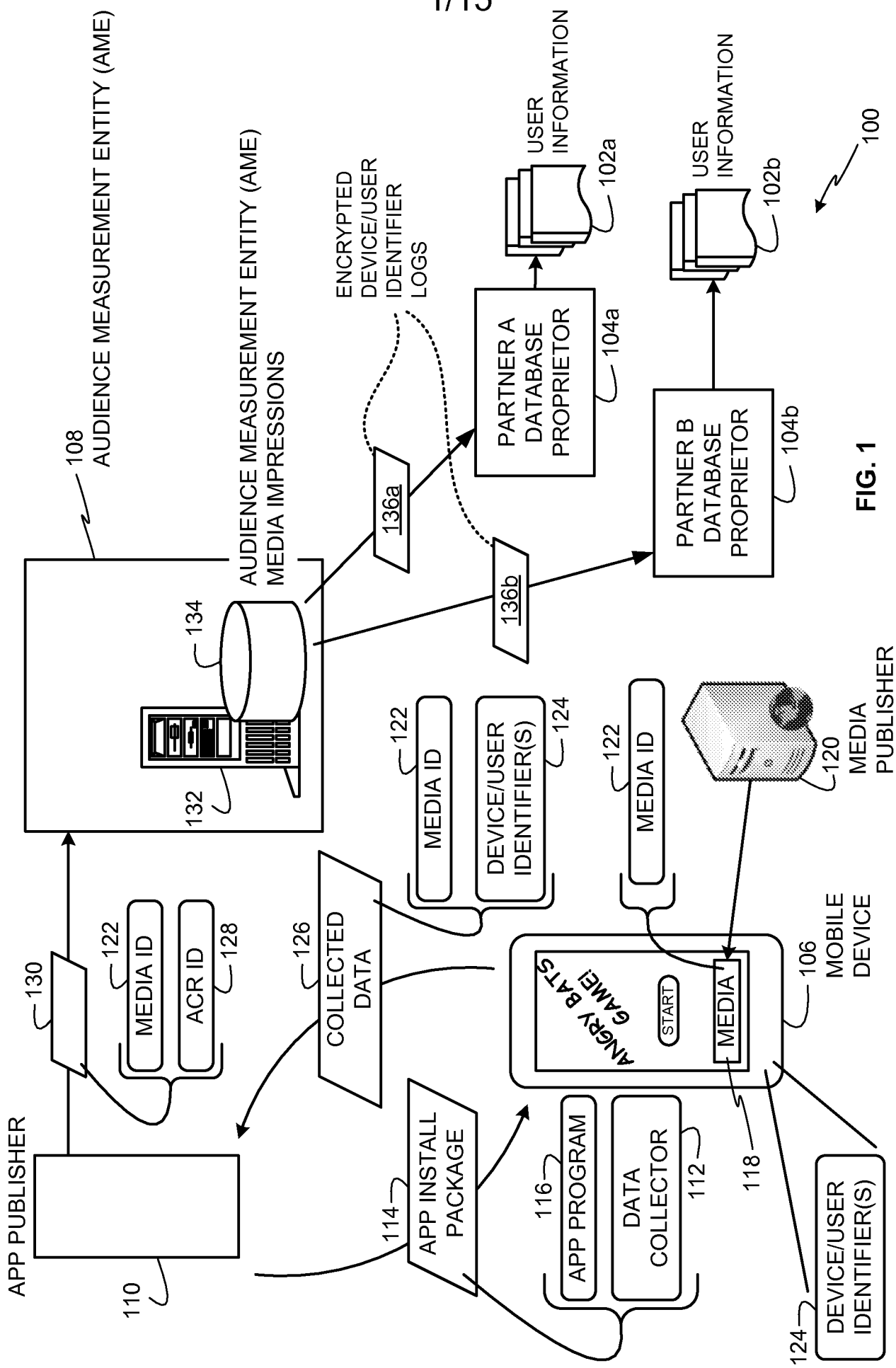

100
108
AUDIENCE MEASUREMENT ENTITY (AME)
AUDIENCE MEASUREMENT ENTITY (AME)
MEDIA IMPRESSIONS
ENCRYPTED DEVICE/USER IDENTIFIER LOGS
USER INFORMATION
102a
USER INFORMATION
102b
PARTNER A DATABASE PROPRIETOR
104a
PARTNER B DATABASE PROPRIETOR
104b
136a
136b
134
132
MEDIA ID
122
DEVICE/USER IDENTIFIER(S)
124
MEDIA ID
122
MEDIA PUBLISHER
120
APP PUBLISHER
110
130
MEDIA ID
122
ACR ID
128
COLLECTED DATA
126
ANGRY BATS GAME!
START
MEDIA
106
MOBILE DEVICE
APP INSTALL PACKAGE
114
APP PROGRAM
116
DATA COLLECTOR
112
118
DEVICE/USER IDENTIFIER(S)
124

FIG. 1

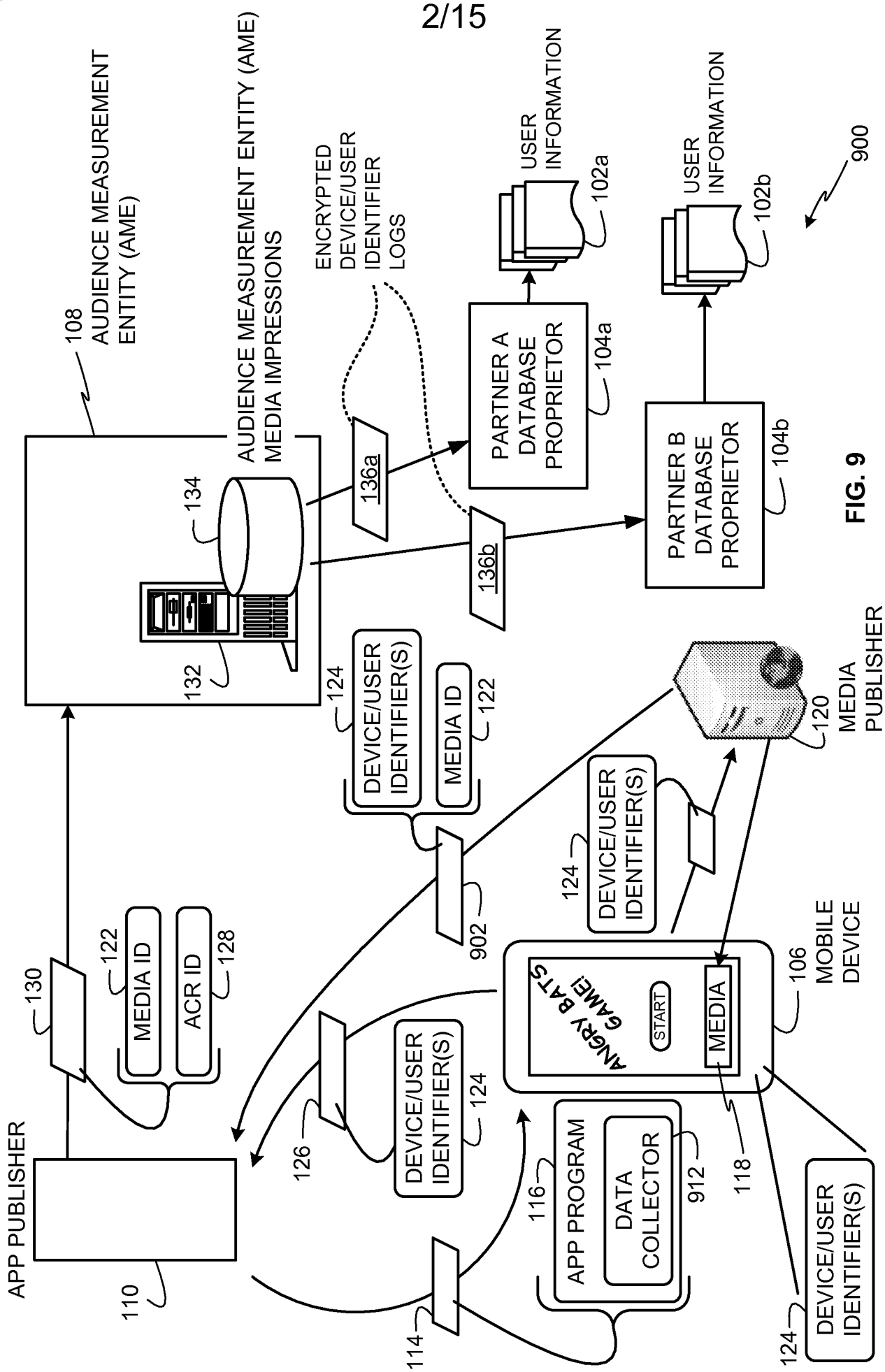

108
AUDIENCE MEASUREMENT ENTITY (AME)
AUDIENCE MEASUREMENT ENTITY (AME) MEDIA IMPRESSIONS
ENCRYPTED DEVICE/USER IDENTIFIER LOGS
USER INFORMATION
102a
USER INFORMATION
102b
900
PARTNER A DATABASE PROPRIETOR
104a
PARTNER B DATABASE PROPRIETOR
104b
134
132
136a
136b
124
DEVICE/USER IDENTIFIER(S)
MEDIA ID
122
120
MEDIA PUBLISHER
902
130
MEDIA ID
122
ACR ID
128
APP PUBLISHER
110
126
DEVICE/USER IDENTIFIER(S)
124
ANGRY BATS GAME!
START
MEDIA
106
MOBILE DEVICE
116
APP PROGRAM
DATA COLLECTOR
912
118
114
DEVICE/USER IDENTIFIER(S)
124

FIG. 9

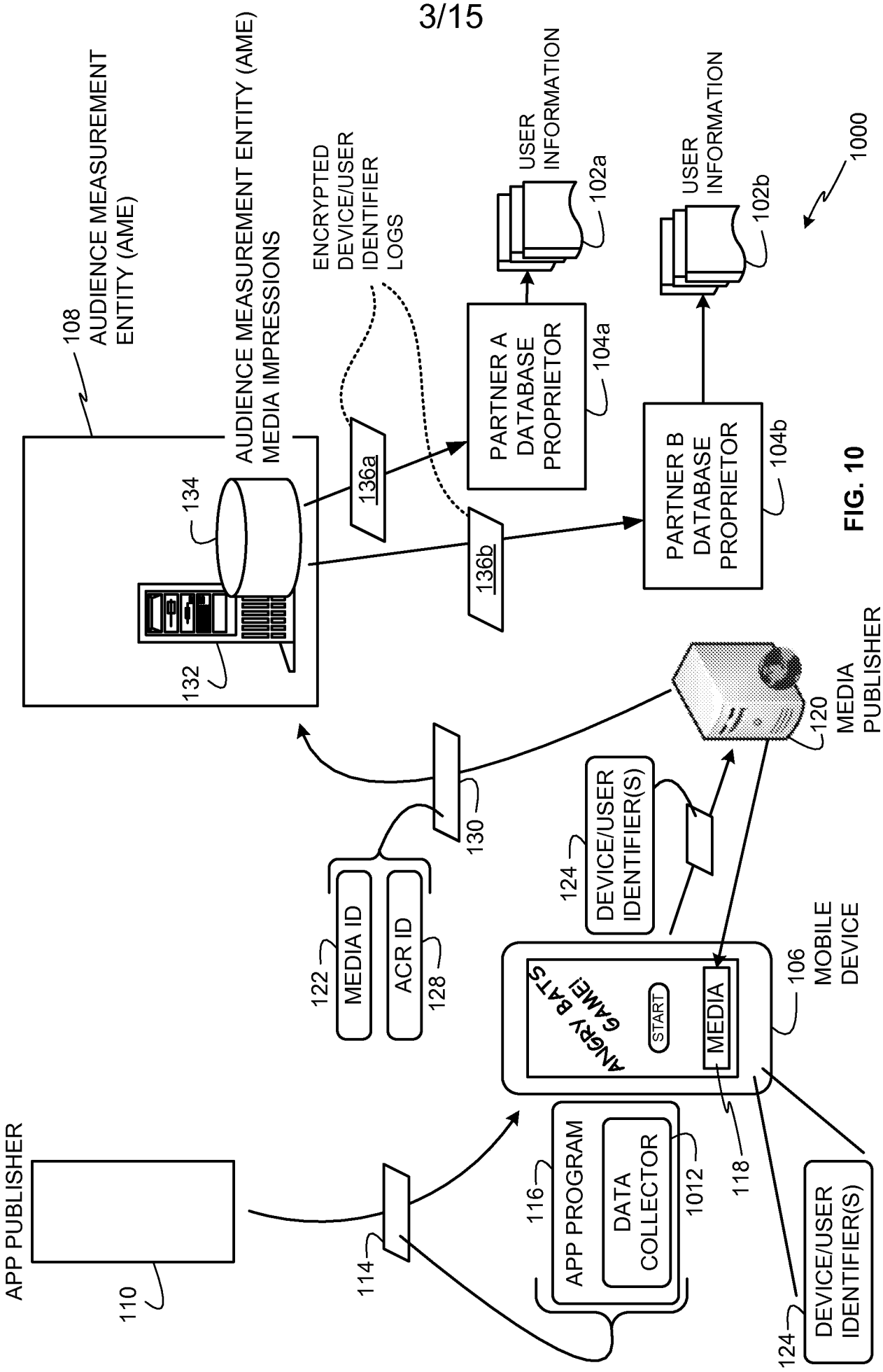

APP PUBLISHER
110
114
APP PROGRAM
116
DATA COLLECTOR
1012
118
DEVICE/USER IDENTIFIER(S)
124
MOBILE DEVICE
106
ANGRY BATS GAME!
START
MEDIA
122
MEDIA ID
128
ACR ID
130
DEVICE/USER IDENTIFIER(S)
124
MEDIA PUBLISHER
120
AUDIENCE MEASUREMENT ENTITY (AME)
108
AUDIENCE MEASUREMENT ENTITY (AME) MEDIA IMPRESSIONS
134
132
136a
136b
ENCRYPTED DEVICE/USER IDENTIFIER LOGS
PARTNER A DATABASE PROPRIETOR
104a
PARTNER B DATABASE PROPRIETOR
104b
USER INFORMATION
102a
USER INFORMATION
102b
1000

FIG. 10

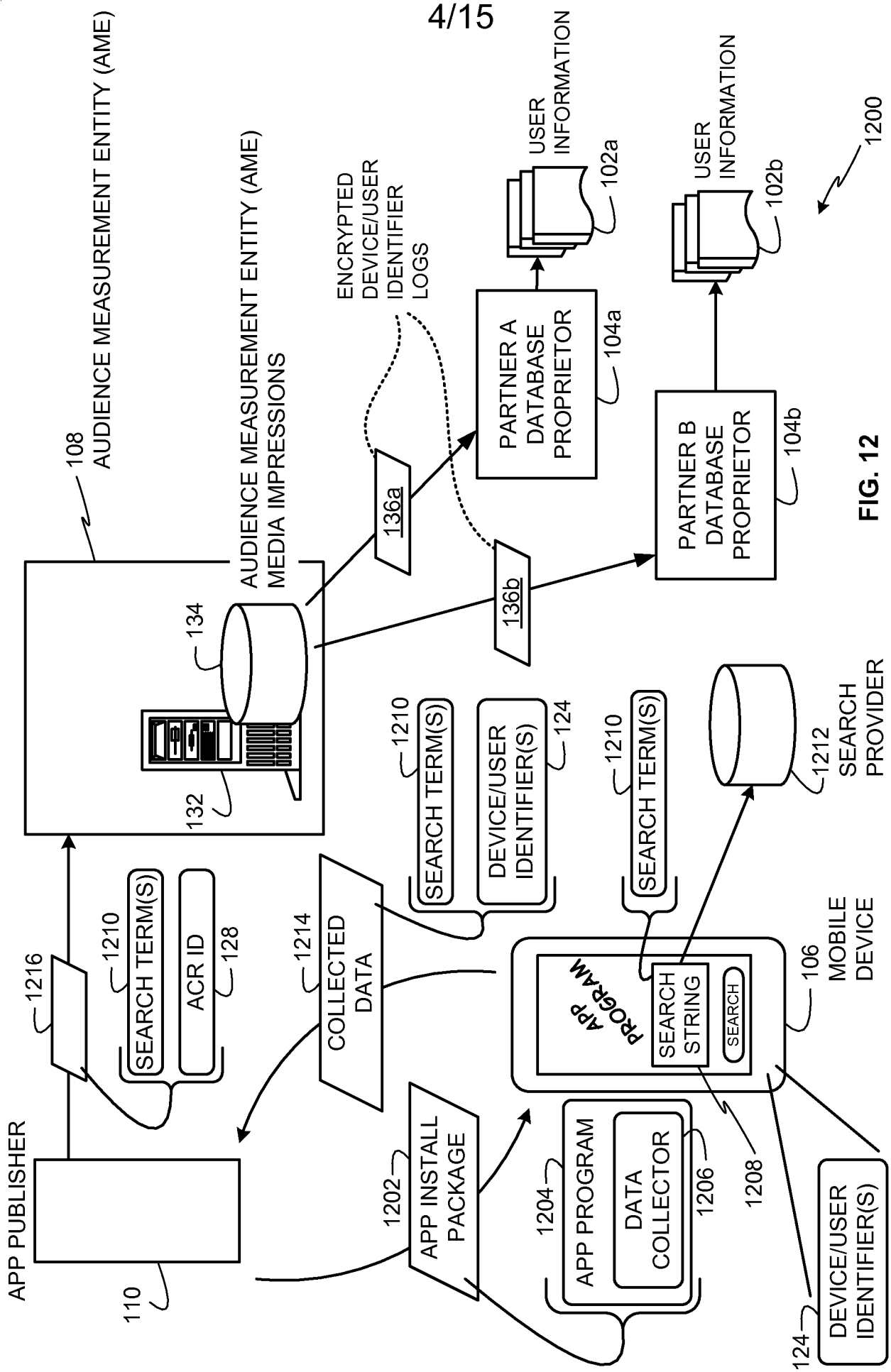

108
AUDIENCE MEASUREMENT ENTITY (AME)
AUDIENCE MEASUREMENT ENTITY (AME)
MEDIA IMPRESSIONS
ENCRYPTED
DEVICE/USER
IDENTIFIER
LOGS
136a
136b
134
132
PARTNER A
DATABASE
PROPRIETOR
104a
PARTNER B
DATABASE
PROPRIETOR
104b
USER
INFORMATION
102a
USER
INFORMATION
102b
1200
1210
SEARCH TERM(S)
DEVICE/USER
IDENTIFIER(S)
124
1210
SEARCH TERM(S)
1212
SEARCH
PROVIDER
1216
1210
SEARCH TERM(S)
ACR ID
128
1214
COLLECTED
DATA
APP
PROGRAM
SEARCH
STRING
SEARCH
106
MOBILE
DEVICE
APP PUBLISHER
110
1202
APP INSTALL
PACKAGE
1204
APP PROGRAM
DATA
COLLECTOR
1206
1208
124
DEVICE/USER
IDENTIFIER(S)

FIG. 12

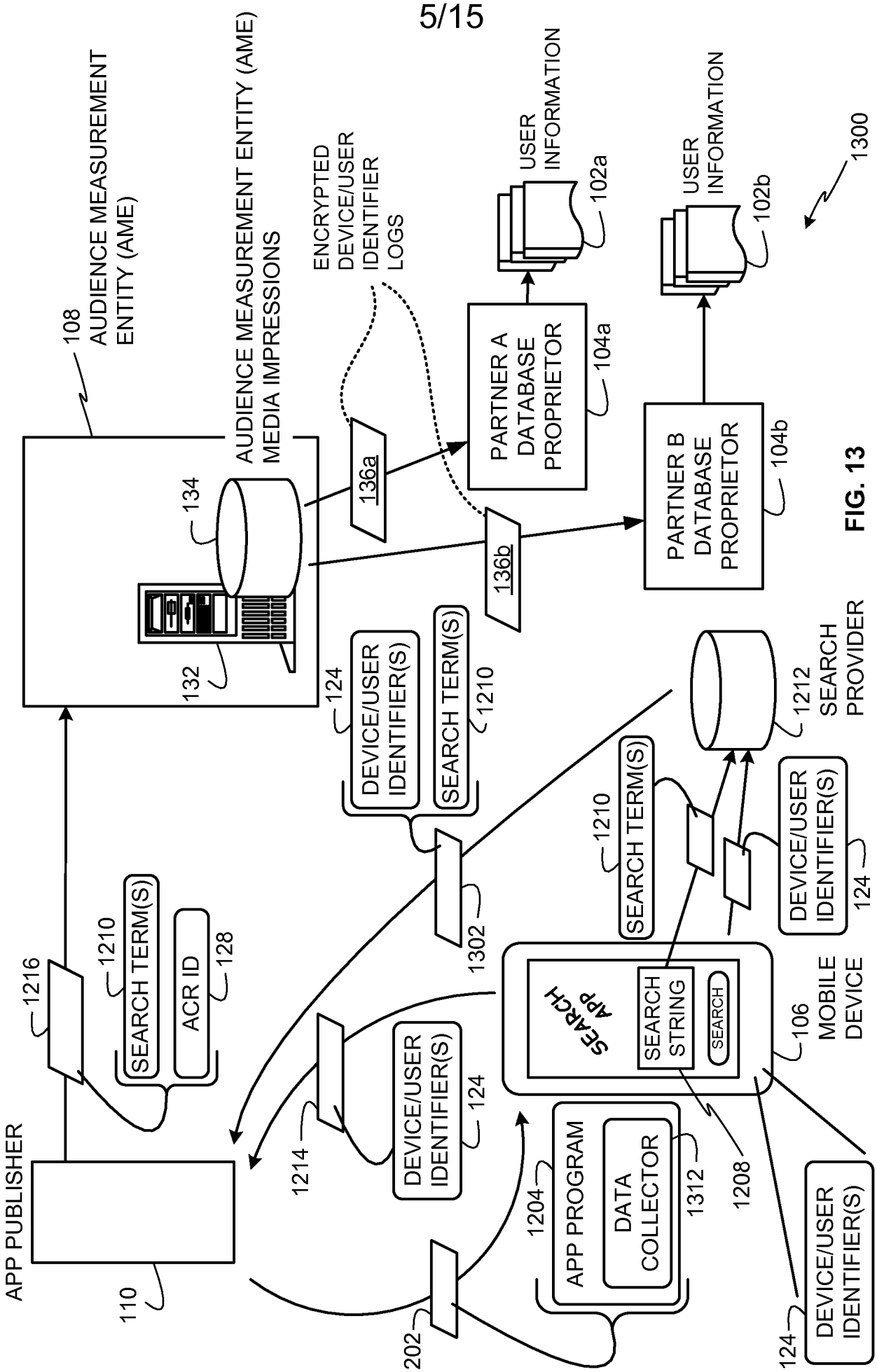

108
AUDIENCE MEASUREMENT ENTITY (AME)
AUDIENCE MEASUREMENT ENTITY (AME) MEDIA IMPRESSIONS
ENCRYPTED DEVICE/USER IDENTIFIER LOGS
USER INFORMATION
102a
USER INFORMATION
102b
1300
PARTNER A DATABASE PROPRIETOR
104a
PARTNER B DATABASE PROPRIETOR
104b
134
132
136a
136b
124
DEVICE/USER IDENTIFIER(S)
1210
SEARCH TERM(S)
1212
SEARCH PROVIDER
1216
1210
SEARCH TERM(S)
ACR ID
128
APP PUBLISHER
110
1302
1214
DEVICE/USER IDENTIFIER(S)
124
SEARCH APP
SEARCH STRING
SEARCH
106
MOBILE DEVICE
1210
SEARCH TERM(S)
DEVICE/USER IDENTIFIER(S)
124
1204
APP PROGRAM
DATA COLLECTOR
1312
1208
1202
124
DEVICE/USER IDENTIFIER(S)

FIG. 13

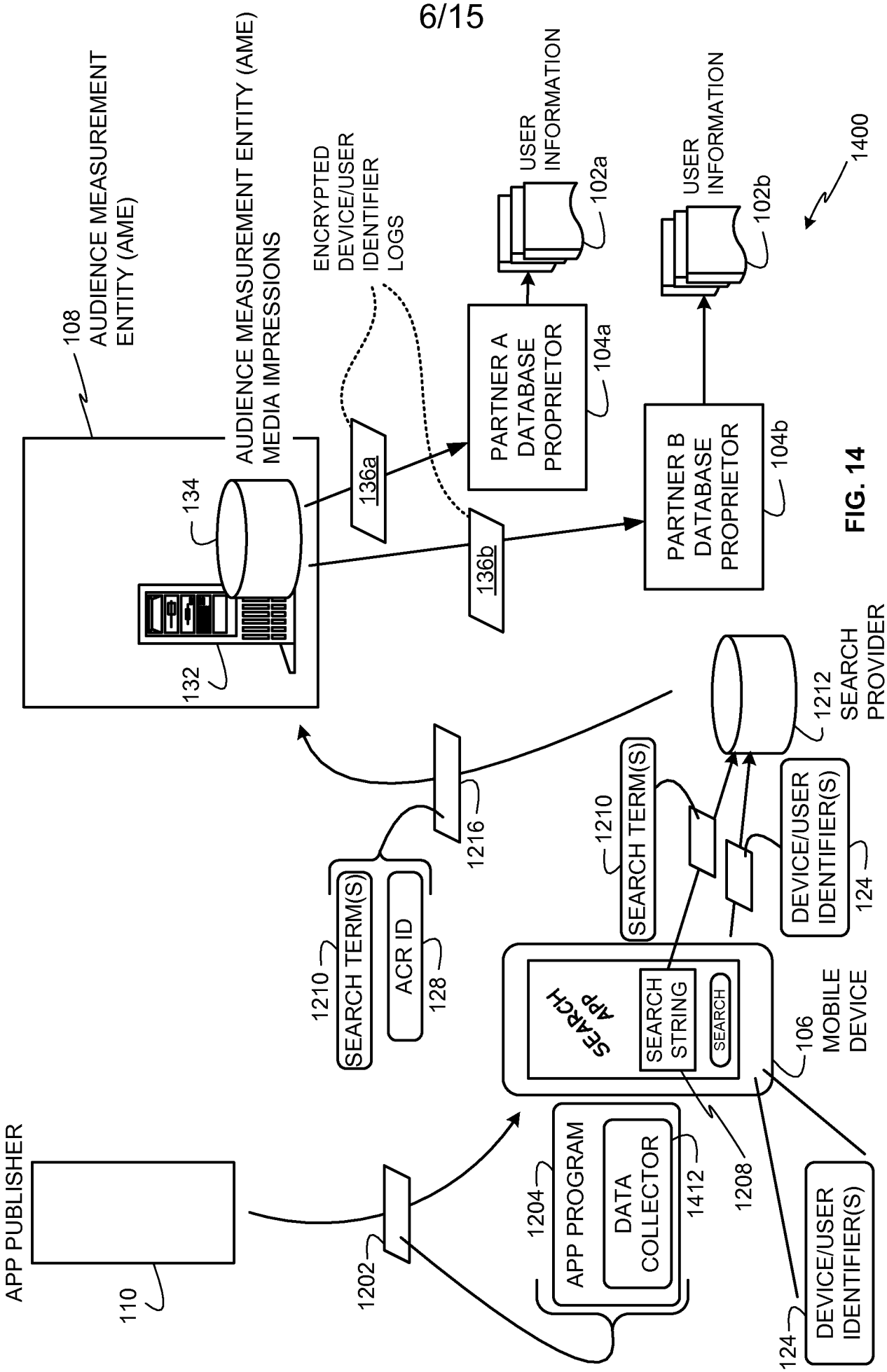

APP PUBLISHER
110
1202
APP PROGRAM
DATA COLLECTOR
1204
1412
1208
DEVICE/USER IDENTIFIER(S)
124
SEARCH APP
SEARCH STRING
SEARCH
106 MOBILE DEVICE
SEARCH TERM(S)
1210
ACR ID
128
1216
1212 SEARCH PROVIDER
SEARCH TERM(S)
1210
DEVICE/USER IDENTIFIER(S)
124
136b
PARTNER B DATABASE PROPRIETOR
104b
USER INFORMATION
102b
PARTNER A DATABASE PROPRIETOR
104a
USER INFORMATION
102a
1400
136a
ENCRYPTED DEVICE/USER IDENTIFIER LOGS
AUDIENCE MEASUREMENT ENTITY (AME) MEDIA IMPRESSIONS
134
132
108 AUDIENCE MEASUREMENT ENTITY (AME)

FIG. 14

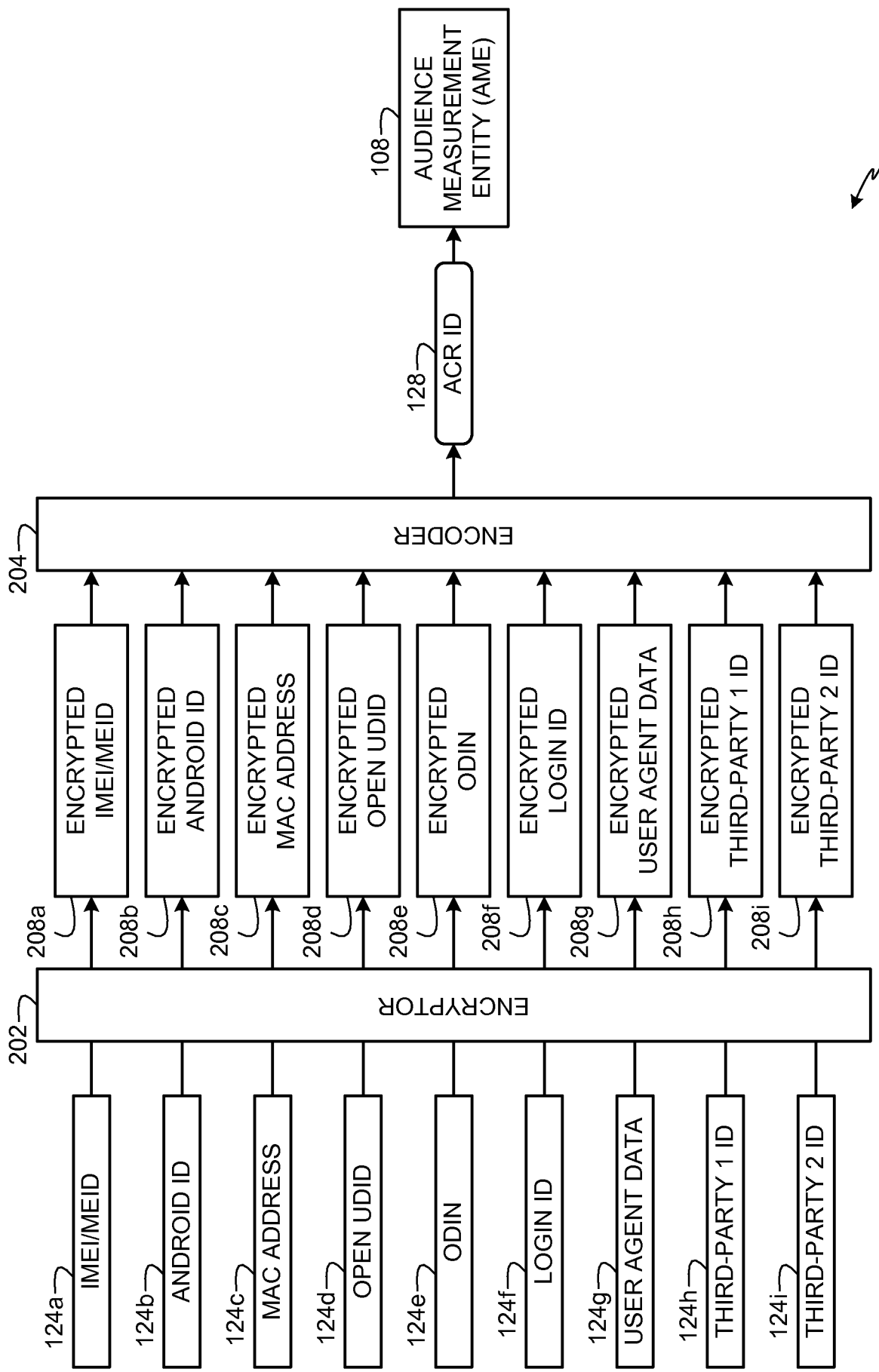

200
108
AUDIENCE MEASUREMENT ENTITY (AME)
128
ACR ID
204
ENCODER
208a
ENCRYPTED IMEI/MEID
208b
ENCRYPTED ANDROID ID
208c
ENCRYPTED MAC ADDRESS
208d
ENCRYPTED OPEN UDID
208e
ENCRYPTED ODIN
208f
ENCRYPTED LOGIN ID
208g
ENCRYPTED USER AGENT DATA
208h
ENCRYPTED THIRD-PARTY 1 ID
208i
ENCRYPTED THIRD-PARTY 2 ID
202
ENCRYPTOR
124a
IMEI/MEID
124b
ANDROID ID
124c
MAC ADDRESS
124d
OPEN UDID
124e
ODIN
124f
LOGIN ID
124g
USER AGENT DATA
124h
THIRD-PARTY 1 ID
124i
THIRD-PARTY 2 ID

FIG. 2

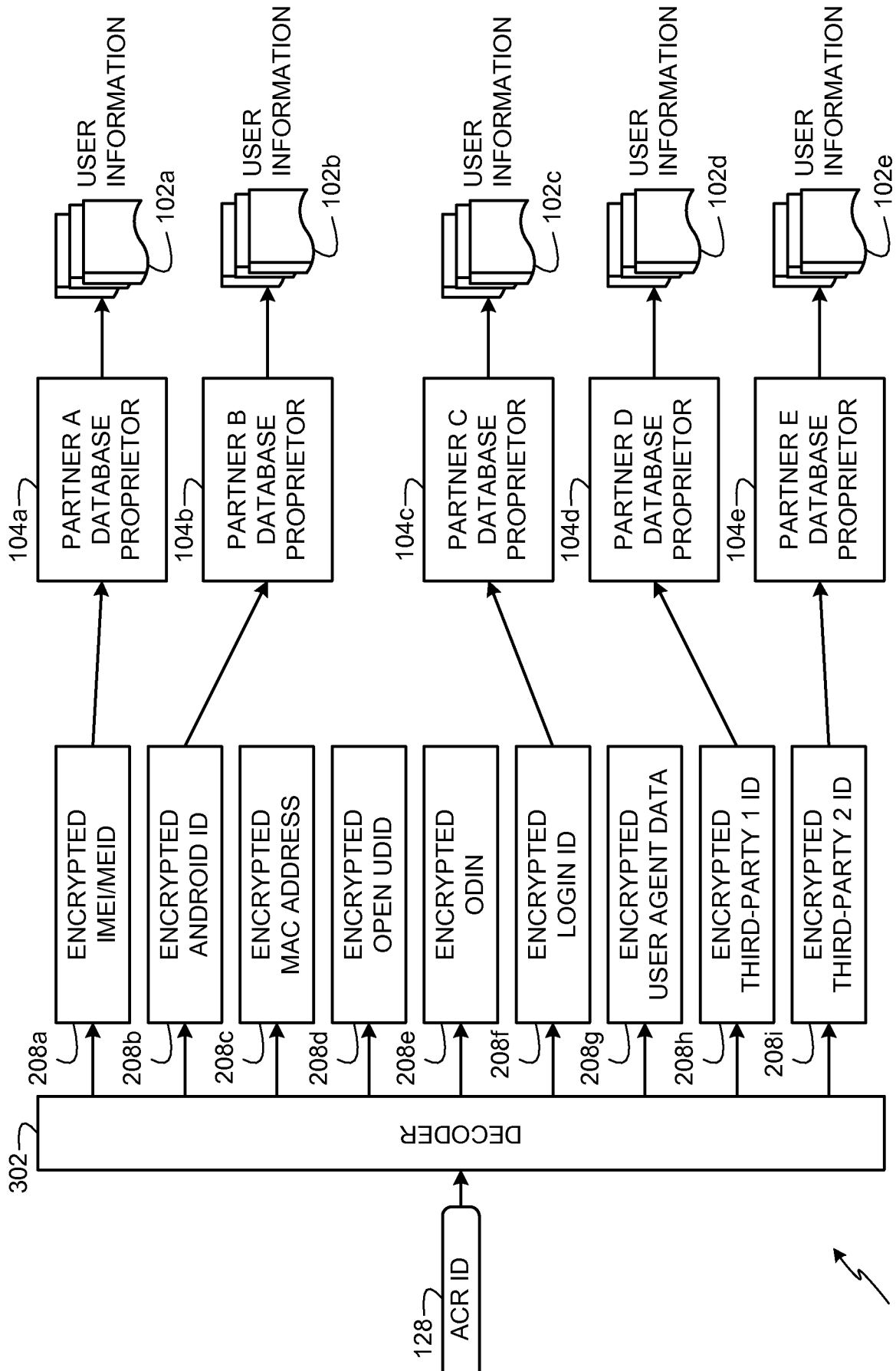

USER INFORMATION
102a
USER INFORMATION
102b
USER INFORMATION
102c
USER INFORMATION
102d
USER INFORMATION
102e
104a
PARTNER A DATABASE PROPRIETOR
104b
PARTNER B DATABASE PROPRIETOR
104c
PARTNER C DATABASE PROPRIETOR
104d
PARTNER D DATABASE PROPRIETOR
104e
PARTNER E DATABASE PROPRIETOR
ENCRYPTED IMEI/MEID
ENCRYPTED ANDROID ID
ENCRYPTED MAC ADDRESS
ENCRYPTED OPEN UDID
ENCRYPTED ODIN
ENCRYPTED LOGIN ID
ENCRYPTED USER AGENT DATA
ENCRYPTED THIRD-PARTY 1 ID
ENCRYPTED THIRD-PARTY 2 ID
208a
208b
208c
208d
208e
208f
208g
208h
208i
302
DECODER
128
ACR ID
300

FIG. 3

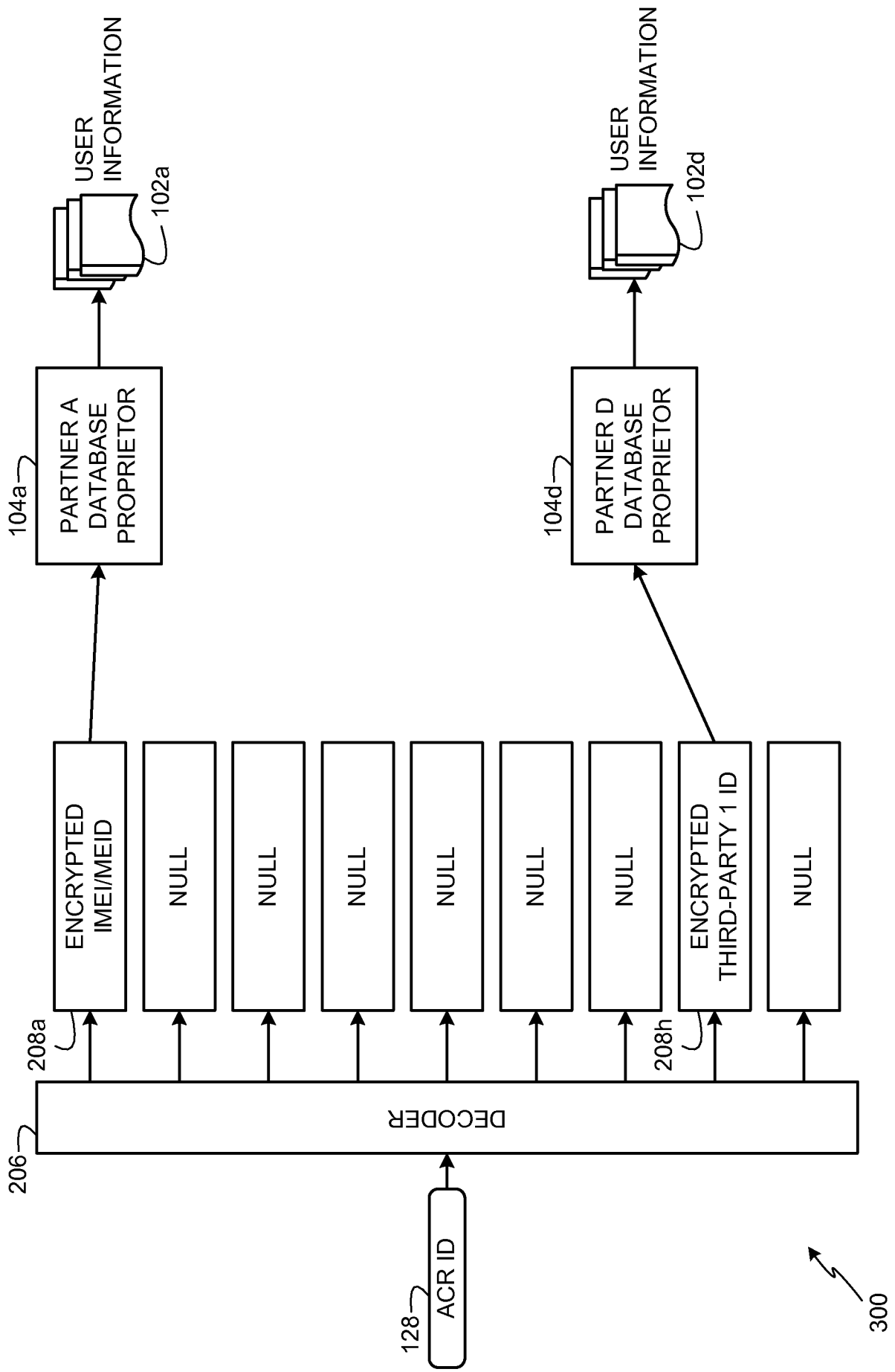

USER INFORMATION
102a
USER INFORMATION
102d
PARTNER A DATABASE PROPRIETOR
104a
PARTNER D DATABASE PROPRIETOR
104d
ENCRYPTED IMEI/MEID
NULL
NULL
NULL
NULL
NULL
NULL
ENCRYPTED THIRD-PARTY 1 ID
NULL
208a
208h
DECODER
206
ACR ID
128
300

FIG. 4

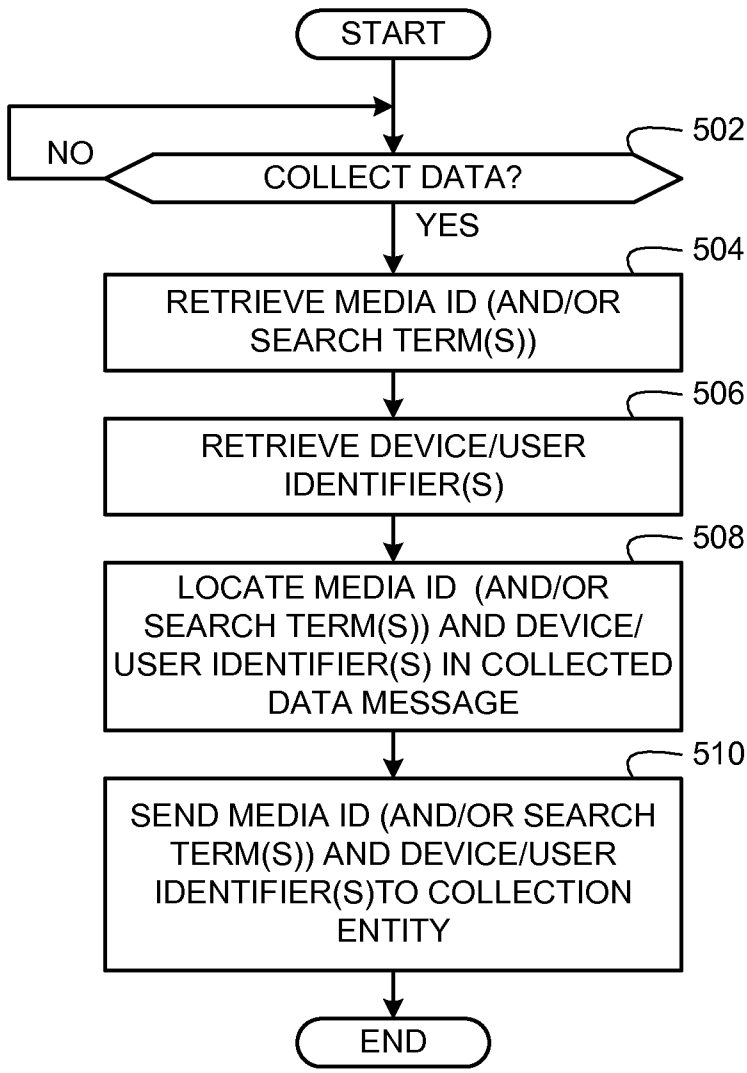

START
NO
502
COLLECT DATA?
YES
504
RETRIEVE MEDIA ID (AND/OR SEARCH TERM(S))
506
RETRIEVE DEVICE/USER IDENTIFIER(S)
508
LOCATE MEDIA ID (AND/OR SEARCH TERM(S)) AND DEVICE/ USER IDENTIFIER(S) IN COLLECTED DATA MESSAGE
510
SEND MEDIA ID (AND/OR SEARCH TERM(S)) AND DEVICE/USER IDENTIFIER(S)TO COLLECTION ENTITY
END

FIG. 5

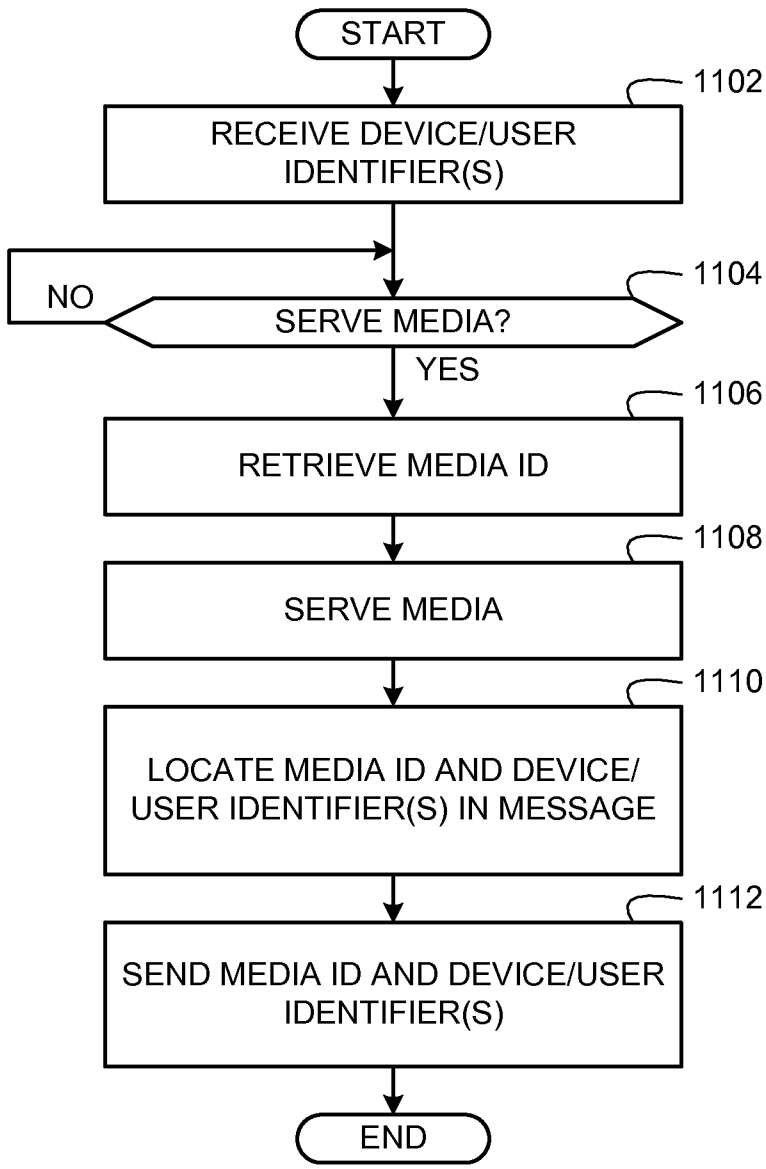

START
1102
RECEIVE DEVICE/USER IDENTIFIER(S)
1104
NO
SERVE MEDIA?
YES
1106
RETRIEVE MEDIA ID
1108
SERVE MEDIA
1110
LOCATE MEDIA ID AND DEVICE/ USER IDENTIFIER(S) IN MESSAGE
1112
SEND MEDIA ID AND DEVICE/USER IDENTIFIER(S)
END

FIG. 11

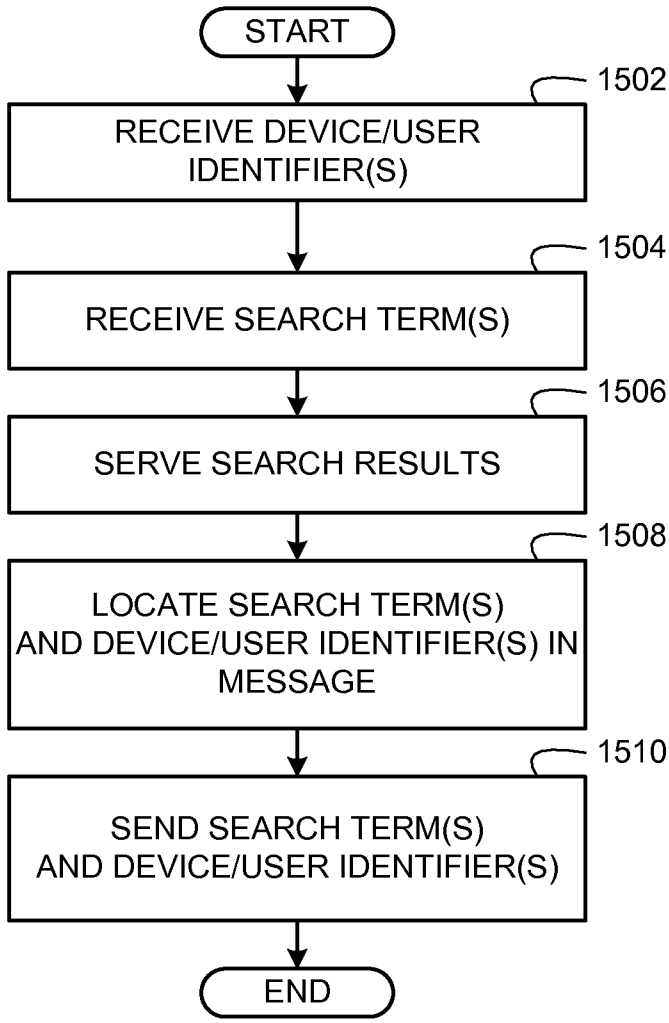

START
1502
RECEIVE DEVICE/USER IDENTIFIER(S)
1504
RECEIVE SEARCH TERM(S)
1506
SERVE SEARCH RESULTS
1508
LOCATE SEARCH TERM(S) AND DEVICE/USER IDENTIFIER(S) IN MESSAGE
1510
SEND SEARCH TERM(S) AND DEVICE/USER IDENTIFIER(S)
END

FIG. 15

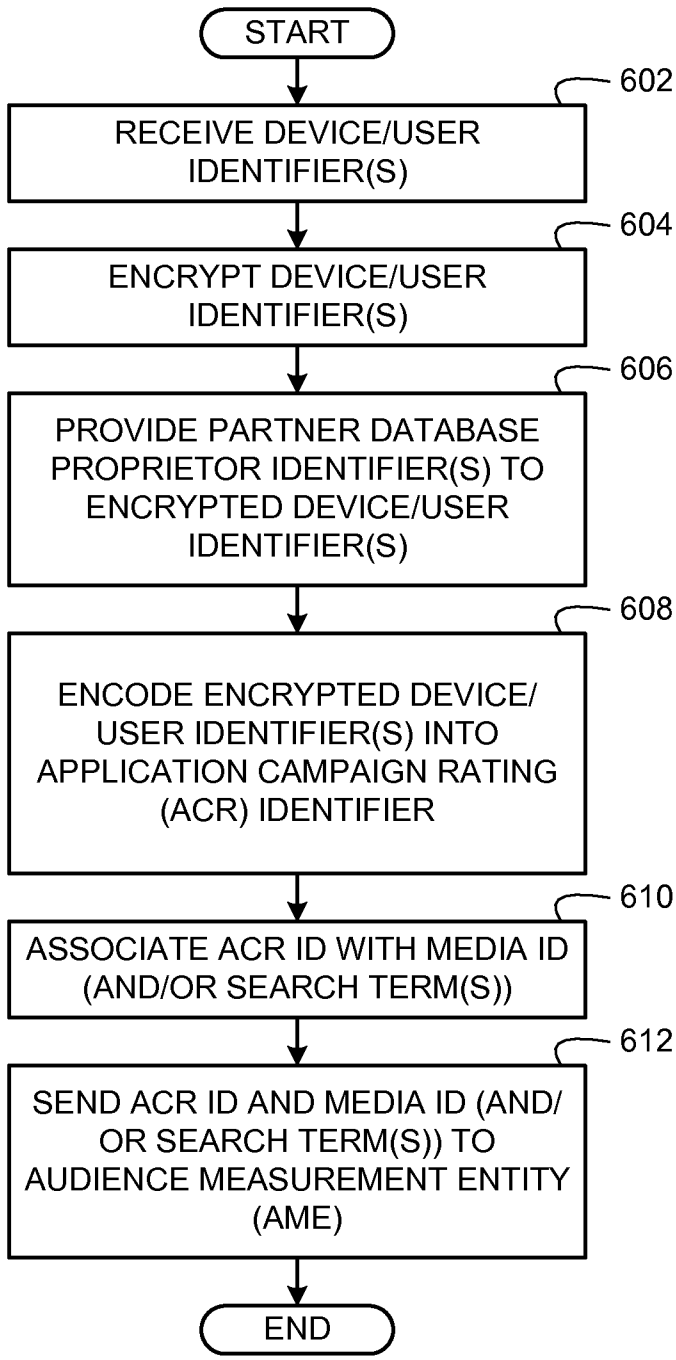

START
602
RECEIVE DEVICE/USER IDENTIFIER(S)
604
ENCRYPT DEVICE/USER IDENTIFIER(S)
606
PROVIDE PARTNER DATABASE PROPRIETOR IDENTIFIER(S) TO ENCRYPTED DEVICE/USER IDENTIFIER(S)
608
ENCODE ENCRYPTED DEVICE/ USER IDENTIFIER(S) INTO APPLICATION CAMPAIGN RATING (ACR) IDENTIFIER
610
ASSOCIATE ACR ID WITH MEDIA ID (AND/OR SEARCH TERM(S))
612
SEND ACR ID AND MEDIA ID (AND/ OR SEARCH TERM(S)) TO AUDIENCE MEASUREMENT ENTITY (AME)
END

FIG. 6

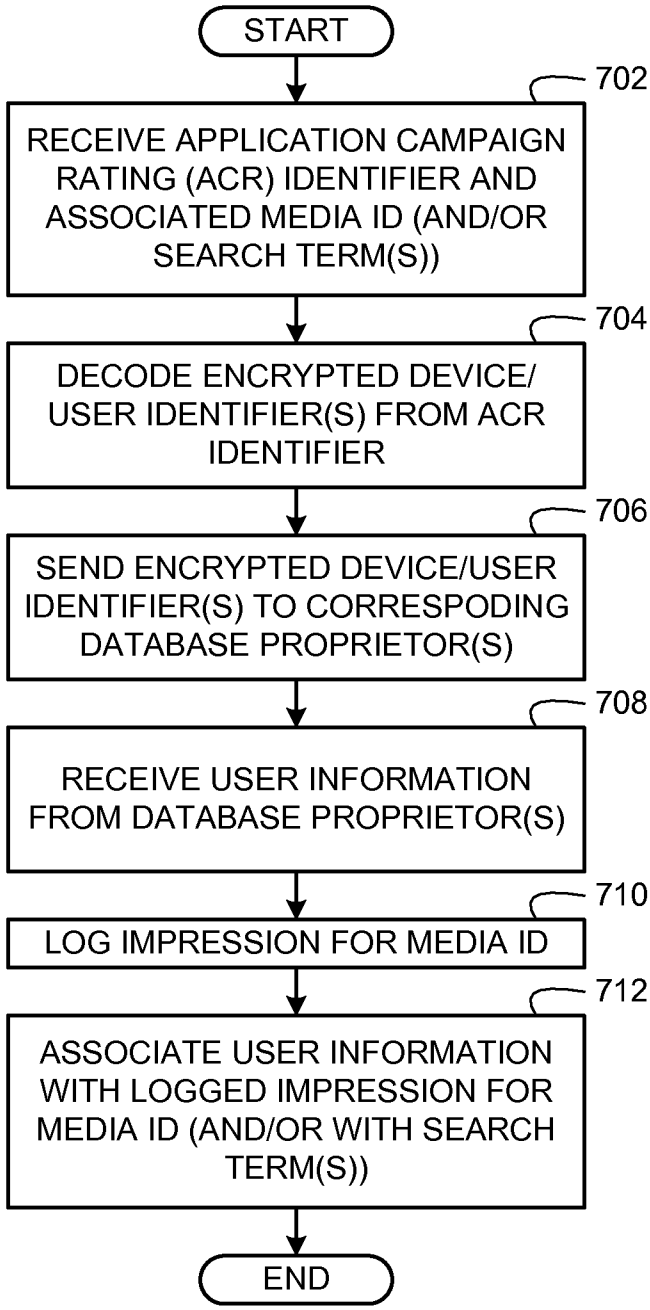

START
702
RECEIVE APPLICATION CAMPAIGN RATING (ACR) IDENTIFIER AND ASSOCIATED MEDIA ID (AND/OR SEARCH TERM(S))
704
DECODE ENCRYPTED DEVICE/ USER IDENTIFIER(S) FROM ACR IDENTIFIER
706
SEND ENCRYPTED DEVICE/USER IDENTIFIER(S) TO CORRESPODING DATABASE PROPRIETOR(S)
708
RECEIVE USER INFORMATION FROM DATABASE PROPRIETOR(S)
710
LOG IMPRESSION FOR MEDIA ID
712
ASSOCIATE USER INFORMATION WITH LOGGED IMPRESSION FOR MEDIA ID (AND/OR WITH SEARCH TERM(S))
END

FIG. 7

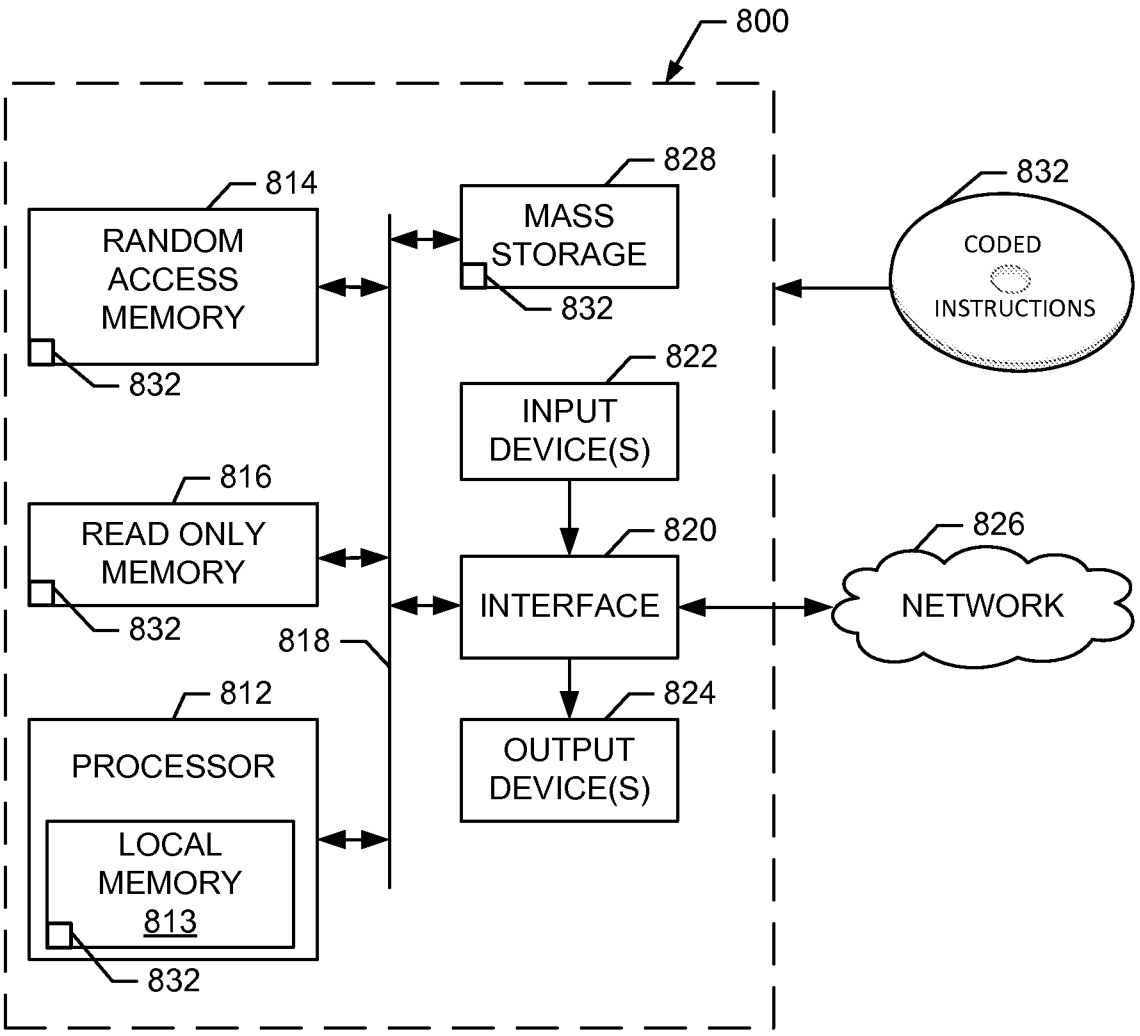
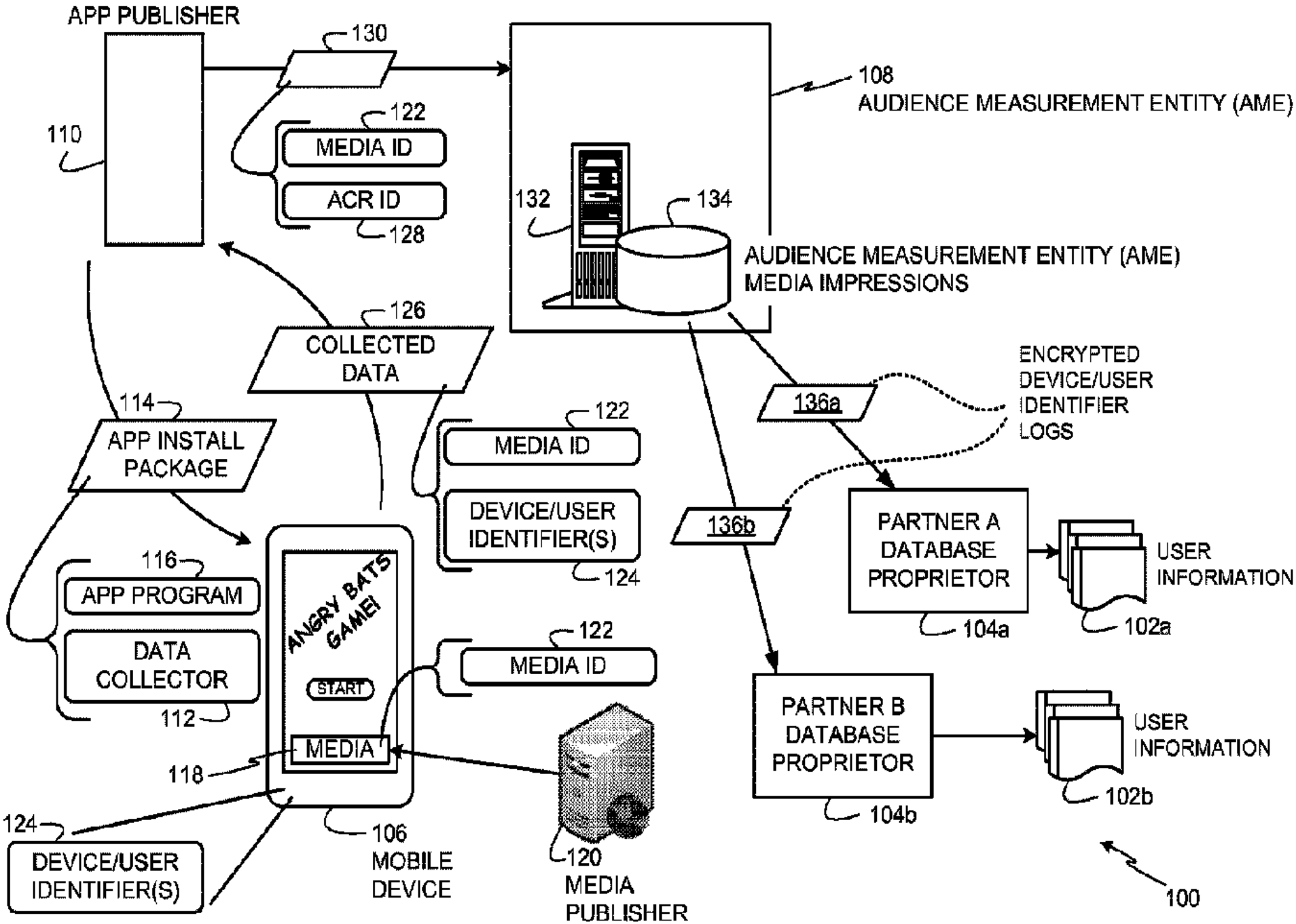

800
814
RANDOM ACCESS MEMORY
832
828
MASS STORAGE
832
832
CODED INSTRUCTIONS
822
INPUT DEVICE(S)
816
READ ONLY MEMORY
832
820
INTERFACE
826
NETWORK
818
812
PROCESSOR
LOCAL MEMORY 813
832
824
OUTPUT DEVICE(S)

FIG. 8


APP PUBLISHER
130
108
AUDIENCE MEASUREMENT ENTITY (AME)
110
122
MEDIA ID
ACR ID
128
132
134
AUDIENCE MEASUREMENT ENTITY (AME)
MEDIA IMPRESSIONS
126
COLLECTED DATA
ENCRYPTED DEVICE/USER IDENTIFIER LOGS
136a
114
APP INSTALL PACKAGE
122
MEDIA ID
DEVICE/USER IDENTIFIER(S)
124
136b
PARTNER A DATABASE PROPRIETOR
USER INFORMATION
104a
102a
116
APP PROGRAM
DATA COLLECTOR
112
ANGRY BATS GAME!
START
MEDIA
118
122
MEDIA ID
PARTNER B DATABASE PROPRIETOR
USER INFORMATION
104b
102b
124
DEVICE/USER IDENTIFIER(S)
106
MOBILE DEVICE
120
MEDIA PUBLISHER
100