(19) **United States**
(12) **Patent Application Publication** (10) **Pub. No.: US 2003/0083938 A1**
Smith et al. (43) **Pub. Date: May 1, 2003**

(54) **SYSTEM AND METHOD FOR PROFILING DIFFERENT USERS HAVING A COMMON COMPUTER IDENTIFIER**

(75) Inventors: **Tucker L. Smith**, Irmo, SC (US); **James L. Browning**, Columbia, SC (US)

Correspondence Address:
JAMES M. STOVER, ESQ.
NCR CORPORATION LAW DEPARTMENT, WHQ-4
1700 S. PATTERSON BOULEVARD
DAYTON,, OH 45479 (US)

(73) Assignee: **NCR Corporation**

(21) Appl. No.: **10/008,259**

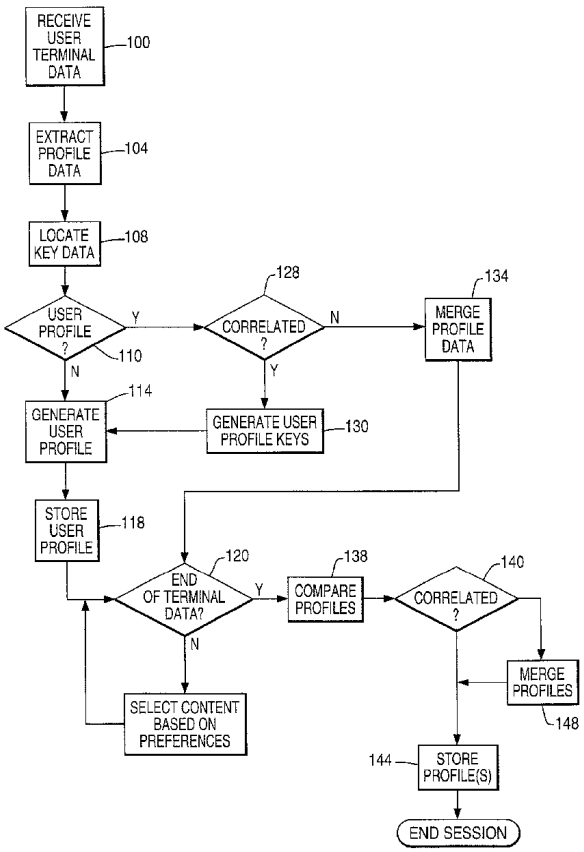
(22) Filed: **Oct. 29, 2001**

Publication Classification

(51) **Int. Cl.**[7] **G06F 17/60**
(52) **U.S. Cl.** **705/14**

(57) **ABSTRACT**

A system and method profiles different users having a common terminal identifier in communication system. The system comprises a user activity data analyzer for extracting profile data from user terminal activity data, a user identifier for determining whether the profile data corresponds to a profile data history associated with the user terminal, and a user profile generator for generating a profile data history from the profile data for another user to be associated with the terminal in response to the profile data not corresponding to the profile data history associated with the user terminal. The user activity data analyzer extracts site addresses, URLs, click event data, metadata and other user activity from a session log to compile information useful for assessing a user's interests. This extracted profile data may then be compared to a profile history previously generated and associated with the terminal identifier. A low level of correspondence between the extracted profile data and the profile history associated with the terminal identifier indicates that a different user is generating the user activity data. The user profile generator then builds a profile history from the extracted profile data and associates it with the terminal identifier. The profile histories are provided different user identifiers. Upon subsequent detection of the terminal identifier, the profile data extracted from the user activity is compared to both profile histories to determine which user is navigating the site. Once sufficient profile data has been extracted to determine which profile history corresponds to the extracted data, advertising content that corresponds to the identified user may be selected and included in the content requested by the current user.



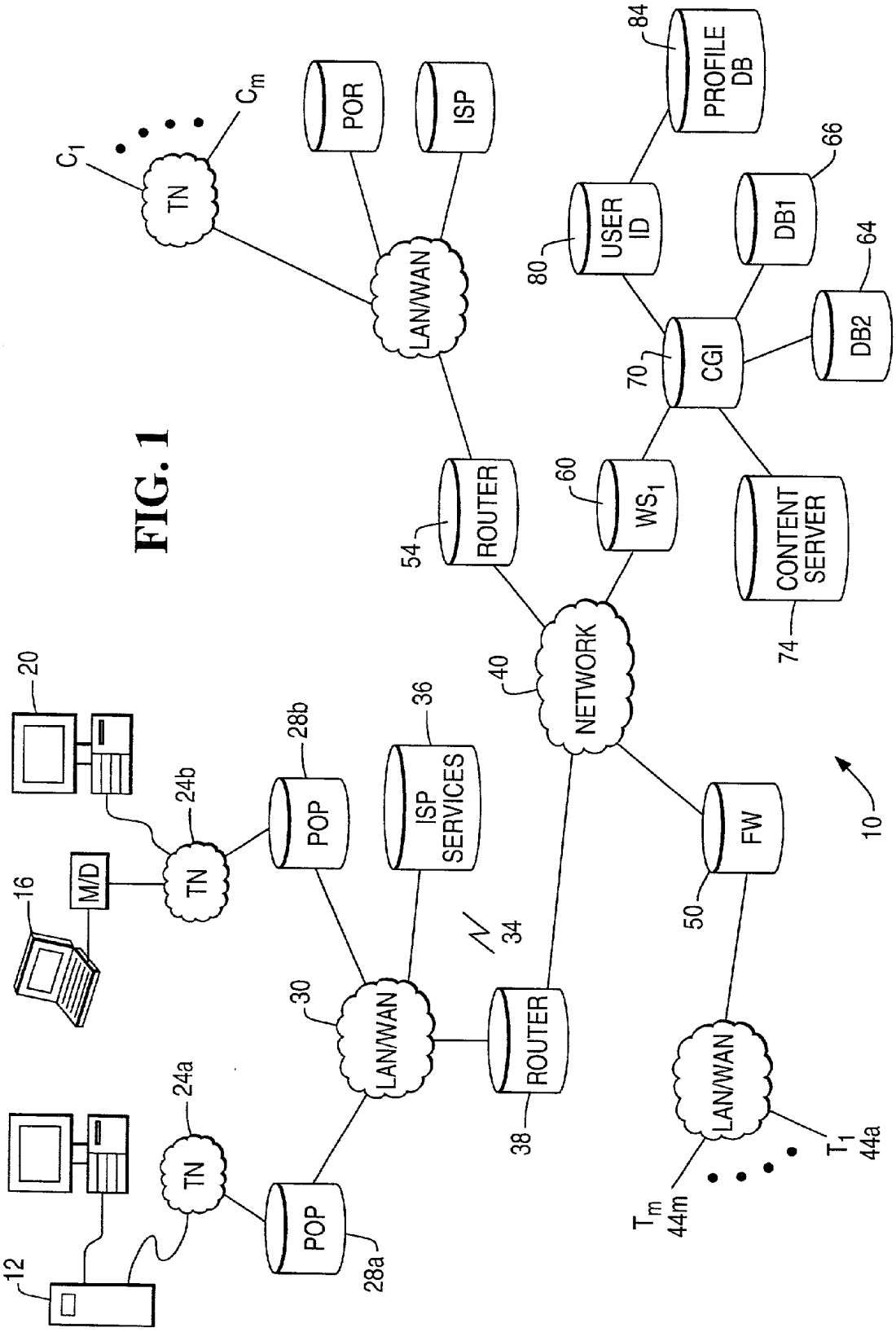


FIG. 1

FIG. 2

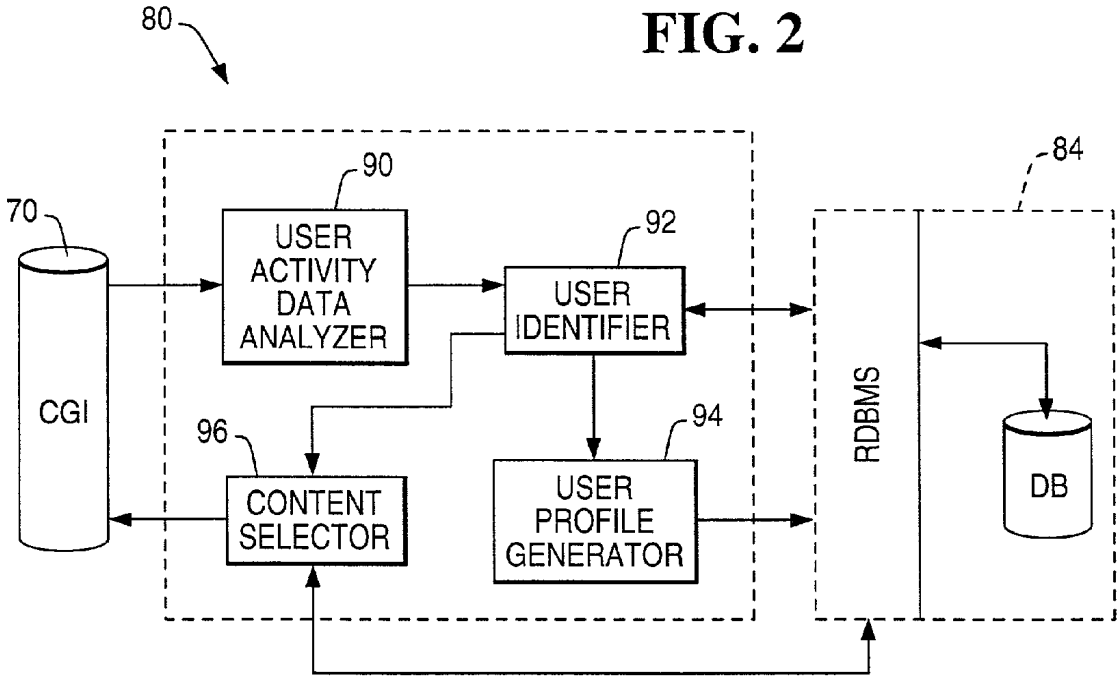
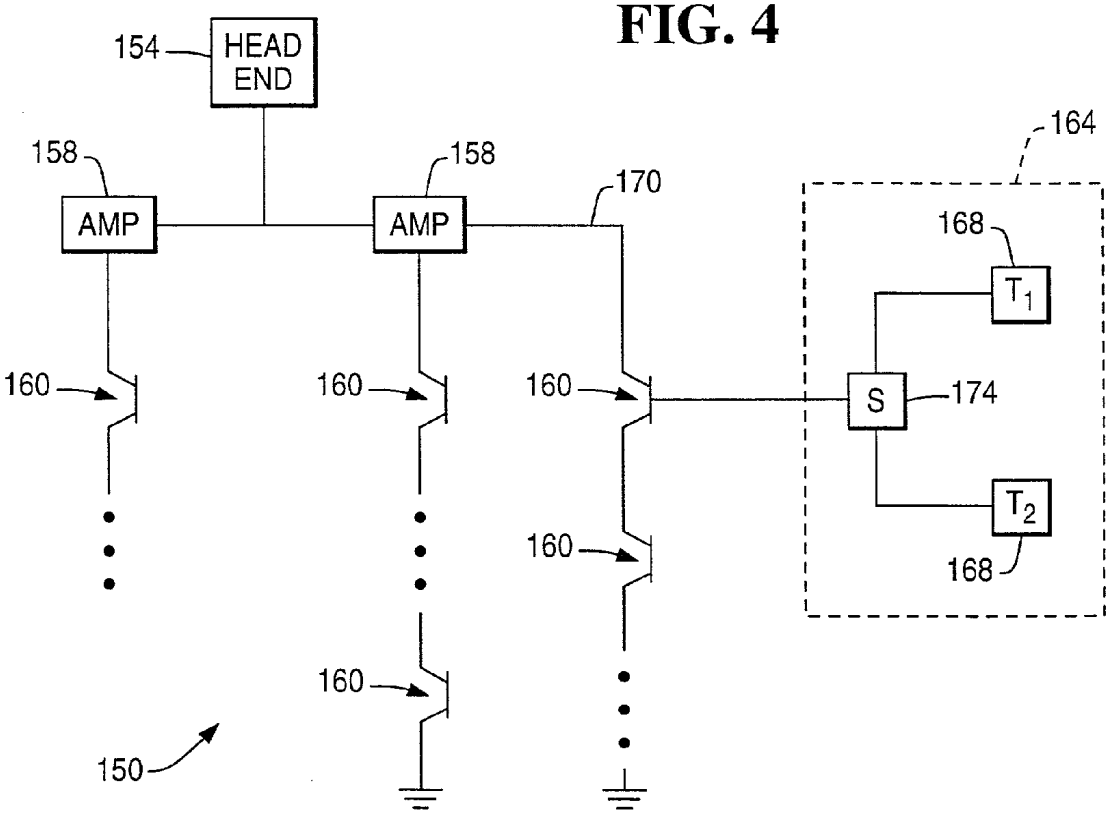


FIG. 4



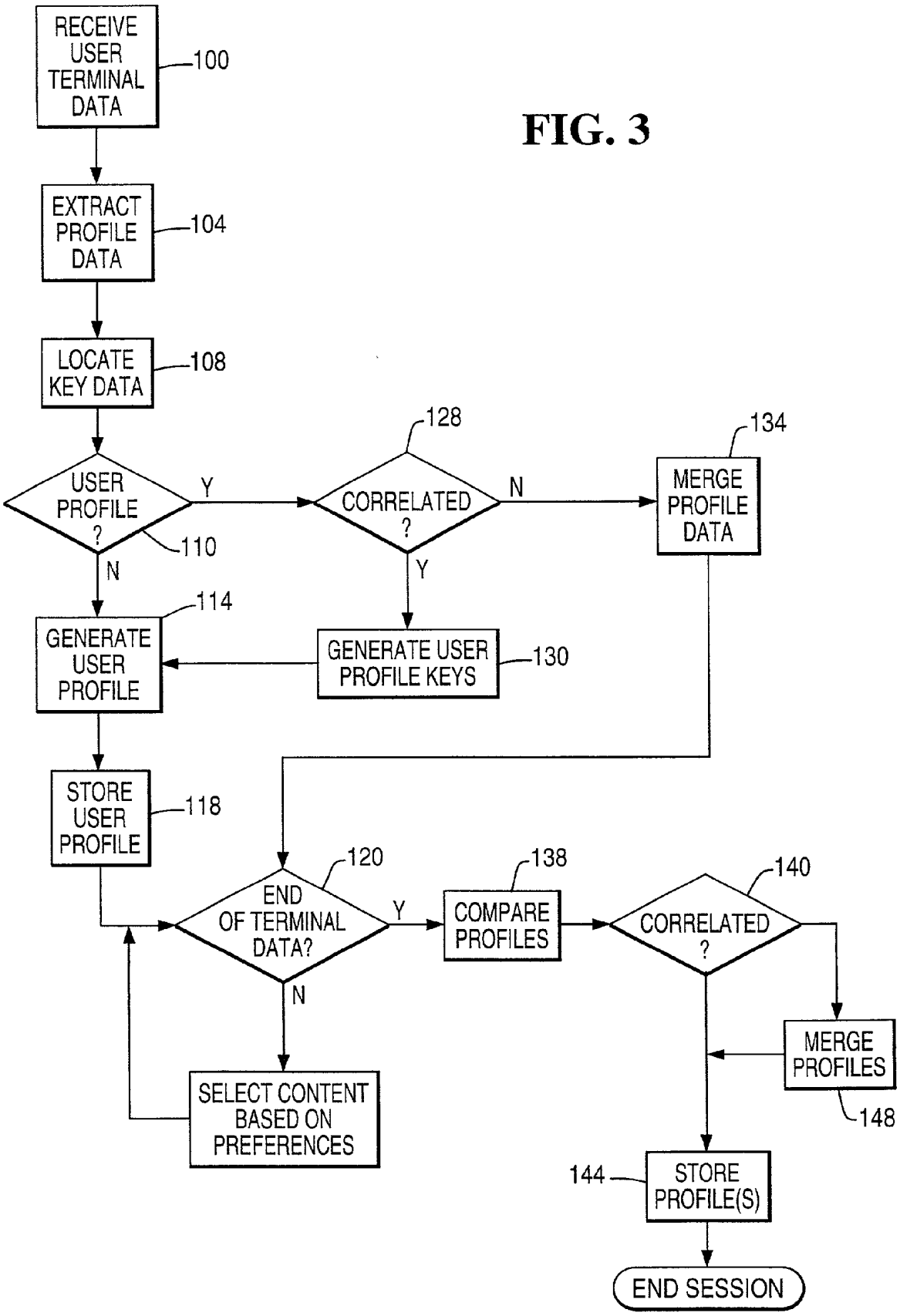


FIG. 3

SYSTEM AND METHOD FOR PROFILING DIFFERENT USERS HAVING A COMMON COMPUTER IDENTIFIER

FIELD OF THE INVENTION

[0001] This invention relates generally to methods and systems for tracking user activity at a terminal on a communication network and, more particularly, to methods and systems for generating user profiles based on user activity a communication terminal.

BACKGROUND OF THE INVENTION

[0002] The Internet is a well-known computer network that supports the interaction of literally millions of computers. Most of these computers communicate through a client/server scheme although the peer-to-peer communication model is used as well. Although the Internet was originally envisioned for the purpose of facilitating the dissemination of information between geographically divergent locations, many have tried to exploit the electronic commerce capability of this network. Few companies, however, have succeeded in establishing commercial viability through revenue generated from sales occurring in Internet electronic transactions alone. Consequently, others have attempted to find a commercial opportunity in the prolific communication traffic that occurs over the Internet for the purposes of information acquisition and dissemination.

[0003] Many Western nations are mass consumer markets and vendors vie for the attention of consumers in order to interest them in their products and/or services. Advertising has moved into every media form as it has arisen, particularly in Western nations, to present products and services to potential consumers in an effort to influence their buying decisions. Advertising agencies and vendors spend significant amounts of resources to learn the attributes that identify those consumers most likely to purchase particular goods and services so the advertising can be placed in the media viewed most often these consumers.

[0004] This targeting of consumers having a high degree of likelihood in purchasing a company's products or services is very important. As the agencies and companies expend significant resources to develop advertising for various media, they want to present them where they are most likely to be effective. For example, car manufacturers do not buy television broadcast time for children's programs and cartoons because the viewers of these shows are not consumers of automobiles. However, cereal manufacturers do purchase this broadcast time because these viewers do influence the buying decisions for breakfast cereals that are made by their parents. Thus, those persons responsible for buying access to media venues are very interested in the persons who view the various media venues.

[0005] The problem with the Internet and indeed any communication network where people are able to view a media anonymously is that little or no knowledge about the demographics of the viewers is known. One particularly frustrating aspect of computer network communication is the inability to identify the computers accessing a server or peer over the network. For example, most users access the Internet through an Internet Service Provider (ISP). In this communication scheme, a user couples to an ISP's communication hub by communicating messages and files through a modem over an analog or digital telephone line. From the ISP's hub, the messages and files may be routed internally through the ISP's intranet to servers or peers that are subscribers to the ISPs services or the messages and files may be routed to the external Internet routers for delivery to servers or peers that are not ISP subscribers. In the message formats for the files and messages, a user's computer includes an Internet Protocol (IP) address to identify the user's computer. However, the ISP typically assigns a different IP address to a computer each time a user accesses the ISP hub and the ISP may change the IP address before sending a message or file out to the external Internet in an effort to cloak the identity of the user's computer. Likewise, computers known as firewalls and secure routers may also alter an IP address for external communications to frustrate efforts to compromise the integrity of a user's computer.

[0006] In an effort to pierce this level of anonymity, some sites utilize the cookie field of Transport Control Protocol/Internet Protocol (TCP/IP) messages. "Cookies," as they have come to be commonly known, are identifiers assigned by a server or peer and placed in reply messages to another computer. Browsers, the application programs for communicating over computer communication networks, particularly those using Hyper Text Transport Protocol (HTTP) for Hyper Text Markup Language (HTML) documents, use the cookie for subsequent messages to the site that assigned the cookie. At the conclusion of a communication session with a site, the communication program, such as a browser, stores the site address and cookie in a file on the user's computer. If the user accesses the site during another subsequent browsing period, the browser determines that the site has been previously accessed by the user and inserts the stored cookie into the messages with the site. If the computer at the site has stored the cookies that it has previously assigned, it can detect the return of a computer that has previously visited. If any information was stored regarding the last time the computer identified by the cookie communicated with the site, then it can be retrieved and used. For example, if the user registered with the site by providing a user name and other user data during the previous visit, then, using the cookie as a key, the site computer can retrieve this data and welcome the user by name without requiring the user to login.

[0007] If users were willing to register on computer sites then advertisers would be able to learn more about the people who visit computer sites. Unfortunately, most users are resistant to providing personal information. Consequently, a site computer may be able to detect the occurrence of another communication session with a computer to which a cookie was previously assigned but little or no information about the user can be ascertained. Not until the user provides personal data in response to a request to complete an information form or performs some transaction that accurately identifies the user will the site be able to obtain demographic data on the user. Once a user's name and/or address can be obtained then personal information databases may be mined to obtain demographic data to further identify the user's interests and attributes.

[0008] Operators of Web sites or other computer sites on computer networks have attempted to exploit the potential of advertising to the users who view content delivered from a site. Site operators try to attract advertisers and vendors by touting the number of "clicks" or "hits" registered at their

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.