US 20040059941A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2004/0059941 A1

Hardman et al. (43) Pub. Date: Mar. 25, 2004

(54) SYSTEMS AND METHODS FOR IDENTIFYING USERS AND PROVIDING ACCESS TO INFORMATION IN A NETWORK ENVIRONMENT

(75) Inventors: **Todd Hardman**, Orem, UT (US); **James Ivie**, Lindon, UT (US); **Michael Mansfield**, Lindon, UT (US); **Greg Parkinson**, Orem, UT (US); **Daren Thayne**, Orem, UT (US); **Mark Wolfgramm**, Provo, UT (US); **Michael Wolfgramm**, Pleasant Grove, UT (US); **Brant Redd**, Provo, UT (US)

Correspondence Address:
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834 (US)

(73) Assignee: **MyFamily.com, Inc.**, Orem, UT

(21) Appl. No.: **10/247,806**

(22) Filed: **Sep. 19, 2002**

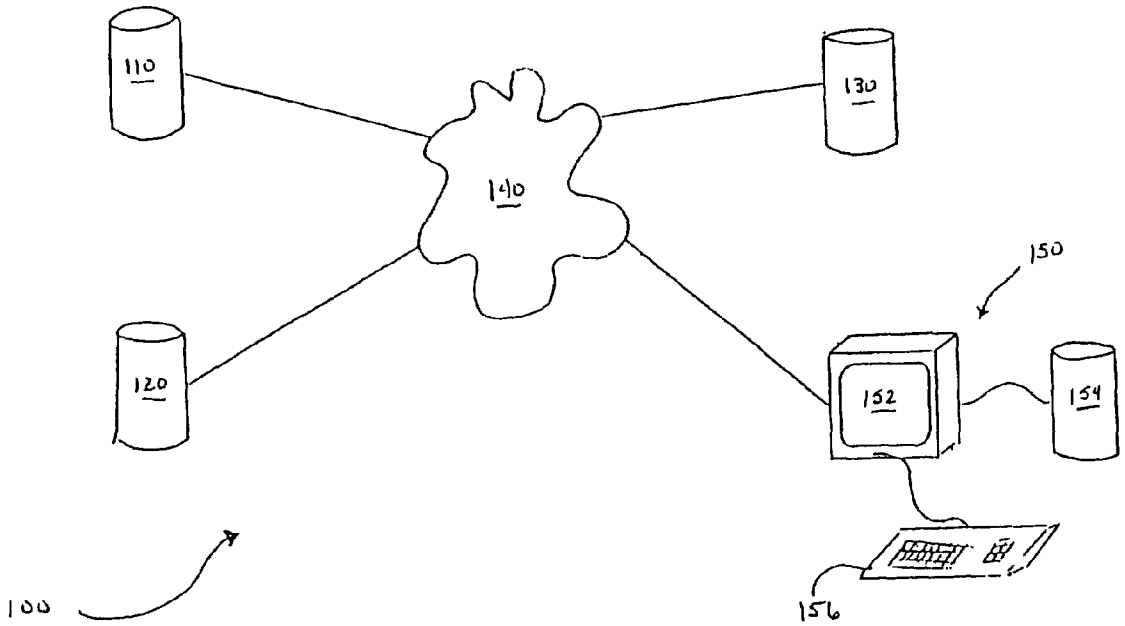
Publication Classification

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **713/201**

(57) **ABSTRACT**

Systems and methods for providing functions from a central facility on a computer network. One function facilitated includes authentication and authorization of users requesting access to a web server accessible via the communication network. Such authorization and authentication includes transferring a request for access from a content server to the central facility and authorizing the request from the central facility. Results of the authorization are communicated to the content server which displays the results of the request to the user by either allowing access or displaying a message describing a denied request.



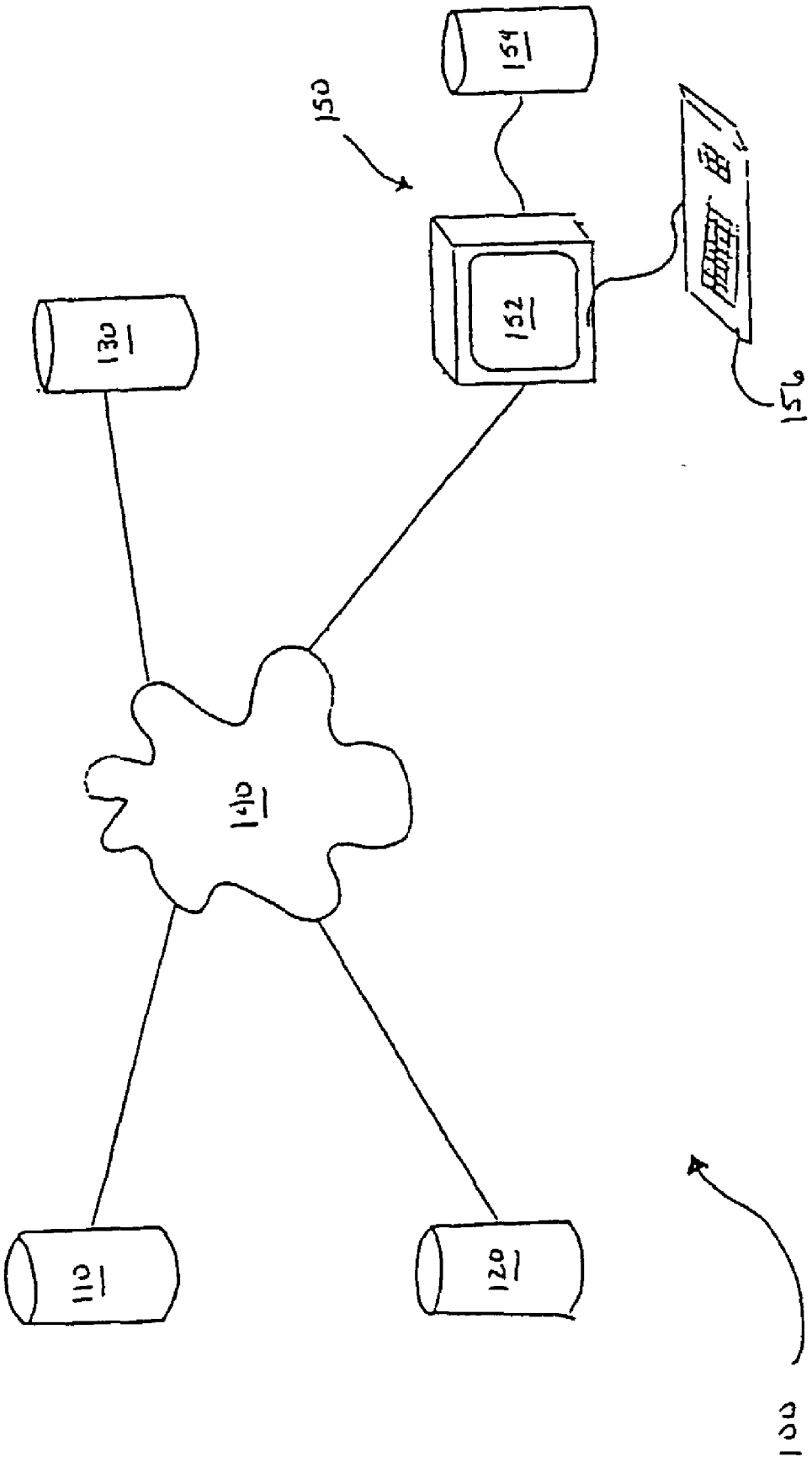


Fig. 1

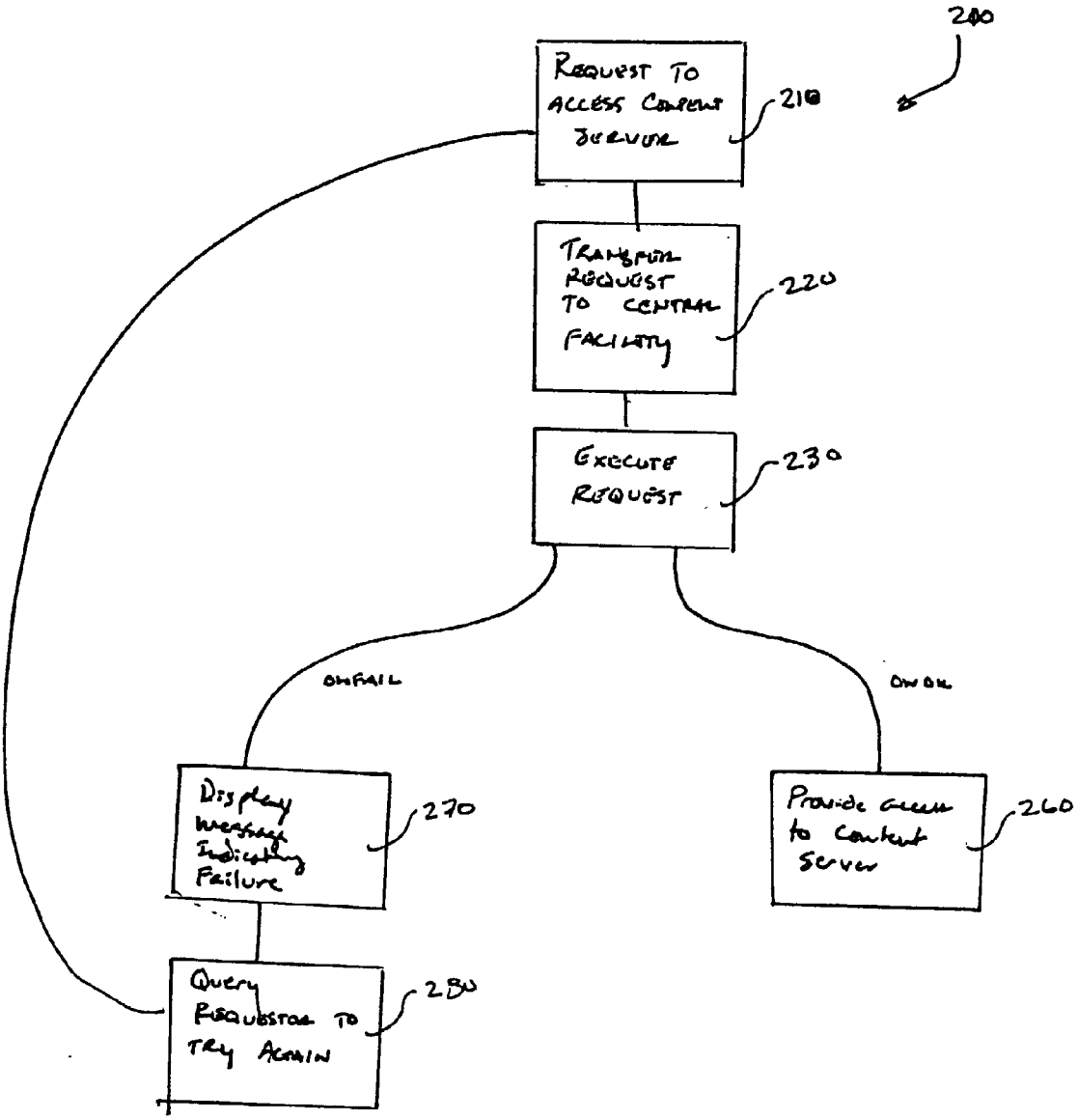


FIG. 2

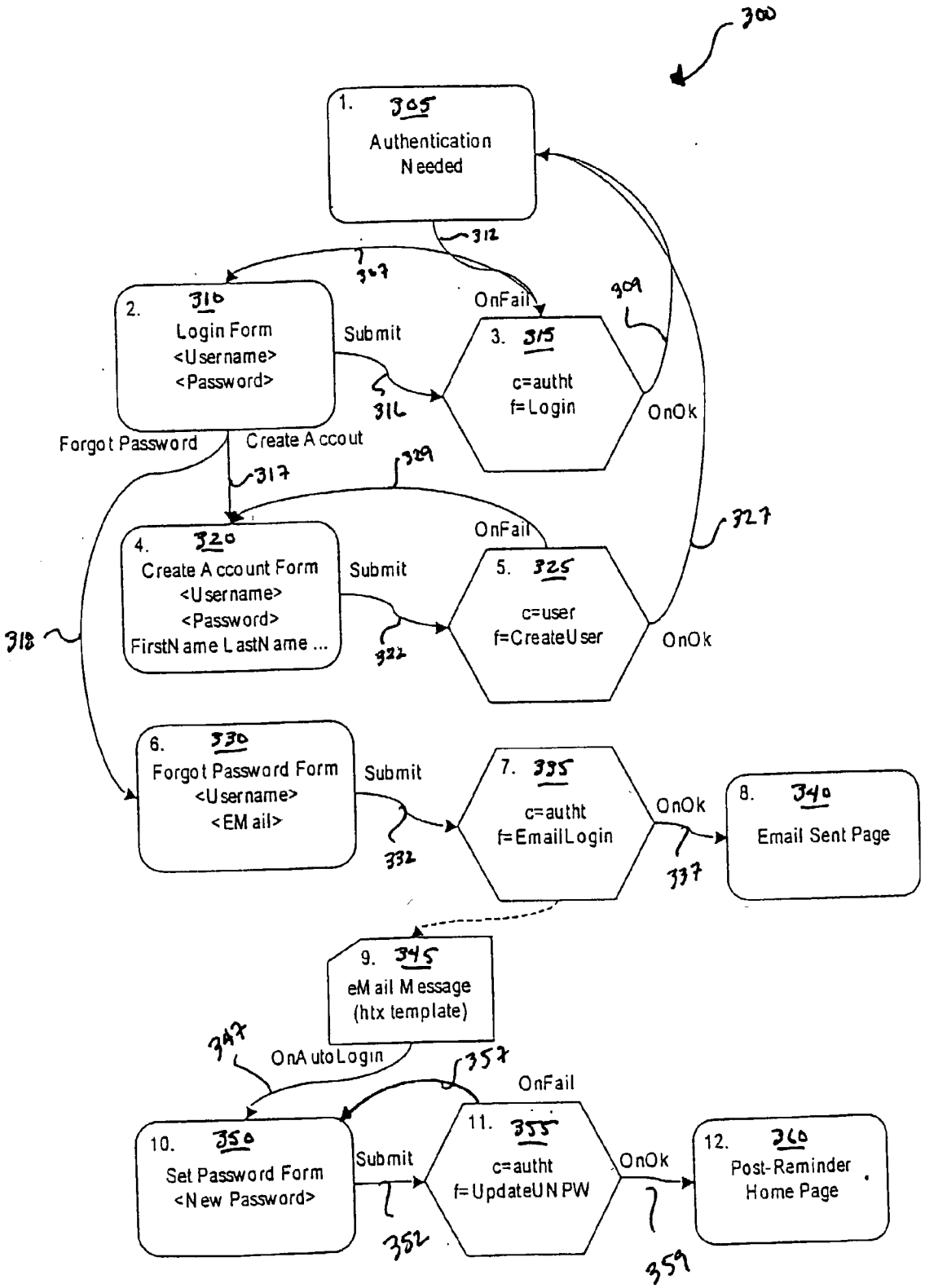


Fig. 3

SYSTEMS AND METHODS FOR IDENTIFYING USERS AND PROVIDING ACCESS TO INFORMATION IN A NETWORK ENVIRONMENT

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is being filed concurrently with related U.S. patent application Ser. No. _____ (Attorney Docket Number 019404-000720US), entitled "SYSTEMS AND METHODS FOR STORING AND RETRIEVING DATA IN A WEB SERVER ENVIRONMENT" and U.S. patent application Ser. No. _____ (Attorney Docket Number 019404-000730US), entitled "SYSTEMS AND METHODS FOR PARTITIONING DATA ON MULTIPLE SERVERS" which are incorporated herein by reference for all purposes.

BACKGROUND OF THE INVENTION

[0002] This invention relates in general to systems and methods for accessing information from a network accessible web server. More specifically, this invention relates to systems and methods for authorizing and authenticating users requesting access to a web server. Yet further, the invention provides systems and methods for facilitating functions provided by a central service on a network.

[0003] Authorization and authentication are typically performed whenever access to a secure web server on a network is requested. In general, such authorization and authentication involves, querying a user for a user name (ID) and password, determining the identity of the user from the queried information, and providing the user with access to a network web server consistent with the user's rights. Upon authentication and authorization, the user is free access the web server associated with the network device.

[0004] This relatively simple approach requires that a user be authenticated and authorized for each secure web server which the user accesses. Thus, for example, a user wishing to access a second web server must again be authenticated and authorized before access to the web server is allowed. This redundancy is useful where a user's access is fundamentally different to the first and second web servers. However, where the two web servers recognize the same user for the same purposes, such redundancy is wasteful.

[0005] One simple solution to eliminate redundancy is to authenticate and authorize a user to access two or more web servers while providing only a single ID and password. For example, a user can be queried when accessing a first web server and upon authentication and authorization can be issued a "cookie" which indicates that the user is authorized to access other related web servers identified by the cookie. Such methods work well when both web servers share first and second level domain names. However, where the first or second level domain names are dissimilar, the method will not work.

[0006] In some instances, web server owners provide authorization and authentication via a central authorization facility often operated by a third party. Thus, for example, when a user accesses a requested web server, the user is redirected to the central authorization facility which queries the user for an ID and a password. Upon authorizing the user, the central authorization facility displays a message indicating status of any authentication and/or authorization. After displaying the message, the central facility redirects the user back to the requested web server.

[0007] In such a system, a user desiring access to a second web server is similarly redirected to the central authorization facility before access to the second web server is allowed. Thus, traffic to the central authorization server is very high. This is particularly inefficient where the user's access to both the first and the second web servers is identical.

[0008] In addition to the inefficiencies, confusing messages are often displayed to users when access to a web server is denied due to either failure of authentication or authorization. Such messages are displayed to the user by the central authorization facility. The messages are confusing because they do not reference the requested web server, but rather reference the central authorization facility. Such messages are particularly confusing to a user that is not aware that they were being redirected for authentication and authorization. In addition to confusing the user, a certain level of brand dilution results from displaying characteristics of the central authorization facility rather than the requested web server.

[0009] To avoid this confusion and brand dilution, many web server owners require the central authorization facility to display a failure message designed by the web server owner. While this alleviates problems with confusion and brand dilution, it is cumbersome and labor intensive. Frequently, providers of the central authorization facility use different tools to author and host their web pages than providers of an associated web server. So, providers of the web server must learn to author using different tools. In addition, whenever a design change is made to the web server, matching changes must be made on the pages served by the central authorization facility.

[0010] Thus, there exists a need in the art for systems and methods for providing third party services, which are transparent to the user. In addition, there exists a need in the art for systems and methods for providing a one time authorization and access to a family of web servers.

BRIEF SUMMARY OF THE INVENTION

[0011] The present invention provides systems and methods for using functions available from a central facility in communication with a computer network. In some embodiments, the functions provided by the central facility include authenticating a user requesting access to a web server. In other embodiments, the functions provided by the central facility include authorizing the user. In addition to authenticating and authorizing a requesting user, the systems and methods of the present invention are applicable to a number of other functions provided by a central facility.

[0012] One embodiment of the present invention includes methods for providing functions from a central facility associated with a computer network. The methods include receiving a request to access a content server. The content server refers at least a portion of the request to the central facility, which executes the request. The results of the execution are indicated to the content server, which in turn displays the results of the request. Because the content server generates the displayed message, any changes to the message can be made without accessing the central facility.

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.