Title: PERSONA DATA STRUCTURE AND SYSTEM FOR MANAGING AND DISTRIBUTING PRIVACY-CONTROLLED DATA

Abstract: A persona data structure for identifying an entity in a network environment. The persona includes a plurality of attributes (301-303). A manager designation is associated with each attribute (301-303), the manager designation identifying an entity that is enabled to set permissions for the attributes (301-303). A permission vector is designated for each attribute (301-303), where the permission vector indicates opt-control preferences set by the attribute’s associated manager. Subsequent distribution of the persona is controlled by the opt-control preferences and manager designations.
PERSONA DATA STRUCTURE AND SYSTEM
FOR MANAGING AND DISTRIBUTING
PRIVACY-CONTROLLED DATA

BACKGROUND OF THE INVENTION

1. Field of the Invention.

The present invention relates, in general, to private data management, and, more particularly, to software, systems and methods for managing privacy controlled data in a distributed computing environment.

2. Relevant Background.

The expansion and convergence of electronic data communication systems offers a seemingly endless number of applications. Applications range from personal communications (e.g., paging, voice and video) to banking, shopping, telecommuting and the like. Essentially any activity that involves communication between individuals, businesses, and machines is impacted by the ubiquitous nature of data communications networks such as the Internet.

Increasingly, business data processing systems, entertainment systems, and personal communications systems are implemented by computers across networks that are interconnected by internetworks (e.g., the Internet). The Internet is rapidly emerging as the preferred system for distributing and exchanging data. Data exchanges support applications including electronic commerce, broadcast and multicast messaging, videoconferencing, gaming, and the like.

Increasingly, electronic communications systems are implemented as distributed computer networks comprising a heterogeneous collection of hardware and software environments operating over a geographically and logically diverse network. Switching technology enables data to traverse
geographic and network boundaries to enable communication between disparate devices. Typically, data is bundled into packets using a packet format or protocol that enables the packet to be routed from a source device to a destination device. A variety of packet routing protocols exist, but a common protocol in use on public networks such as the Internet is Internet protocol (IP).

The Internet is a collection of disparate computers and networks coupled together by a web of interconnections using standardized communications protocols. The Internet is characterized by its vast reach as a result of its wide and increasing availability and easy access protocols. Although other communication network technologies and protocols are available including wireless networks, fibre channel, and the like, the Internet is readily adapted to include these and other technologies.

Unfortunately, the nature of digital data lends itself to easy storage, copying and distribution of data communicated over a digital communication system. This raises significant privacy concerns on the part of network users. One of the more significant challenges to be overcome in gaining acceptance of electronic commerce systems is gaining confidence in the privacy in digital communications.

Every time a browser communicates with an intranet Web site information is shared about the user with the sites that are visited in exchange for information, products and services. Web sites share information with the user as well. Desirably the personal information that is shared should be securely locked away and only shared in conformance with user desires. Internet experiences can be greatly enhanced by the use of personal information. When a browser visits web sites that are enable to use the personal information the Web experience can be more personalized as well as convenient. Shopping and obtaining information is faster and easier because the personal information allows forms to be automatically filled out. However, each time personal information is shared with a web site the user must cross that the web site owner has a privacy policy in place and will only used to
personalization data in compliance with a privacy policy. It is convenient to study and analyze each privacy policy of each web site. Hence, most users are not aware of how the personal information will be used. A need exists for a convenient, robust, extensible mechanism for sharing and securing personal data in an Internet environment.

The desires for privacy militate against the advantages of personalization that electronic commerce can provide. Personalization refers generally to the process of customizing a digital communication (e.g., web page, order form, advertisement, e-mail, voice mail and the like) based upon a user's personal information. While advertising, marketing, and commerce in general throughout the industrial era has concentrated on mass, impersonal communication, the historical roots of commerce lie in very personalized communication between customers, merchants, and third parties. Personalization is generally preferred by both businesses and individuals as it promises to limit unwanted advertising, offer more desirable products, and reduce distribution costs among other advantages. However, personalization requires that personal information be gathered, stored, organized and used in digital form in a manner that raises privacy concerns. A need exists for mechanisms, methods and systems for handling privacy information in a manner that promotes confidence and security while enabling efficient use of the private data.

In terms of the Internet, an "infomediary" is a Web site or other Internet-based entity that provides specialized information for exchange between producers of goods and services and their potential customers. Any consumer e-commerce site that provides information as well as an order form could be classed as an infomediary. Infomediaries facilitate this business-to-business and business-to-consumer data traffic.

Internet protocols define small data storage elements called "cookies" for storing state information. Cookies are specified in RFC 2109 produced by the Internet Engineering task force (IETF). Cookies were designed to enable
stateful sessions in a normally stateless Internet environment using hypertext transfer protocol (HTTP) requests and responses. Cookies are small data structures created by a web site and stored persistently on a user's machine. Cookies are widely used to store personalization information such as names, shopping preferences, credit card information, and the like. RFC 2109 places stringent, inflexible privacy controls on the use of cookies by requiring client browser software to restrict how information stored in cookies is transmitted from the browser. For example, a cookie can only be accessed by a web site in the same domain as the server that wrote the cookie initially, thereby preventing sharing of cookies between web sites.

Current protocols prevent users from easily manipulating the contents of a cookie or from controlling distribution of the data stored in cookies. The only way users can readily manage cookies is to prevent them being written to the user's machine or delete them after they are written. Furthermore, cookies are not shared amongst user machines so that a similar information is stored on each machine used to access a web site. In view of the trend towards users accessing network resources using a larger number and variety of network appliances, this duplication of information and effort becomes burdensome. Further, because cookies are stored persistently on the user's machine(s) they are subject to manipulation and attack by hackers. As this private information is stored on more and different kinds of machine, the risk of unauthorized access to this private information increases dramatically. Accordingly, a need exists for a system, method and protocol for managing personal information that is both secure and yet readily shared according to user-specified permissions.

SUMMARY OF THE INVENTION

A persona data structure for identifying an entity in a network environment. The persona includes a plurality of attributes. A manager designation is associated with each attribute, the manager designation identifying an entity that is enabled to set permissions for the attributes. A
permission vector is designated for each attribute, where the permission vector indicates opt-control preferences set by the attribute's associated manager. Subsequent distribution of the persona is controlled by the opt-control preferences and manager designations.

**BRIEF DESCRIPTION OF THE DRAWINGS**

Fig. 1 shows a distributed computer environment in which the present invention is implemented;

Fig. 2A illustrates a distributed computing and information exchange environment in which the present invention is implemented;

Fig. 2B shows a more specific electronic commerce environment in which the present invention is implemented;

Fig. 3 illustrates an exemplary data structure for holding persona data;

Fig. 4 and Fig. 5 show exemplary extensible markup language implementations of a persona data structure in accordance with the present invention; and

Fig. 6 illustrates an alternative implementation of a privacy server in accordance with the present invention.

**DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS**

The present invention is illustrated and described in terms of a distributed computing environment such as an enterprise computing system using public communication channels such as the Internet. However, an important feature of the present invention is that it is readily scaled upwardly and downwardly to meet the needs of a particular application. Accordingly, unless specified to the contrary the present invention is applicable to
significantly larger, more complex network environments as well as small network environments such as conventional LAN systems.

FIG. 1 shows an exemplary computing environment 100 in which the present invention may be implemented. Environment 100 includes a plurality of local networks such as Ethernet network 102 and FDDI network 103. Any number of network architectures, topologies and technologies may be used to implement local networks including Token ring, Appletalk, fibre channel and the like. Individual client machines are coupled through LANs 102 and 103 and/or through an internet service provider (ISP) 110 to network 101. LANS 102/103, as well as individual clients 107, may use hardware such as router 109 to enable connection to network 101. In the environment shown in FIG. 1, a number of computing devices and groups of devices are interconnected through network 101. LANs 102 and 103 may be implemented using any available topology and may implement one or more server technologies including, for example a UNIX, Novell, or Windows NT, or peer-to-peer type network. Each network will include distributed storage implemented in each device and typically includes some mass storage device coupled to or managed by a server computer.

Local networks 102, 103 and 104 include one or more workstations such as client computers 107. One or more computers 107 may be configured as an application and/or file server. Computers 107 typically include a data processor, memory, input/output (I/O) devices a local storage for executing computer programs. In accordance with the present invention, client computers 107 implement a user interface such as a Web browser that supports markup-language formats such as hypertext markup language (HTML), extensible markup language (XML), universal markup language (UML) and the like. In the preferred implementations the browser supports active content using Java and/or ActiveX technology. Network communication with a web browser is implemented using HTTP. Each LAN 102/103 may include a number of shared devices (not shown) such as printers, file servers, mass storage and the like.
Each of the devices shown in FIG. 1 may include memory, mass storage, and a degree of data processing capability sufficient to manage their connection to network 101. The computer program devices in accordance with the present invention are implemented in the memory of the various devices shown in FIG. 1 and enabled by the data processing capability of the devices shown in FIG. 1. In addition to local memory and storage associated with each device, it is often desirable to provide one or more locations of shared storage such as disk farm 116 that provides mass storage capacity beyond what an individual device can efficiently use and manage. Selected components of the present invention may be stored in or implemented in shared mass.

Network 101 comprises, for example, a public network such as the Internet or another network mechanism such as a fibre channel fabric or conventional WAN technologies. Network 101 includes a wide variety of interoperable, geographically distributed hardware such as switches, hubs, concentrators, and routers. Network services for routing data and configuring network hardware can be implemented in both the network hardware itself as well as shared resources such as servers 111. Servers implement a wide variety of services such as domain name servers for translating domain names into qualified network addresses, file servers, directory servers, search engine services and the like.

Fig. 2A and Fig. 2B illustrate principle functional components in accordance with the present invention. FIG. 2B is a more specific implementation of the components shown in FIG. 2A. The system shown in Fig. 2A and FIG. 2B implements a new type of privacy-enhanced relationship between a network appliance 200, a network resource such as commerce web site 210, and a privacy engine 220. The system shown in Fig. 2A and FIG. 2B leverages existing network mechanisms and protocols to enable a privacy relationship that give a user operating network appliance 200 control over the kind of personal data that is exchanged as well as which web sites 210 are able to access the data.
The privacy enhanced features of the present invention are provided by the managed exchange of data structures, called " personas" (indicated by an encircled "P" in Fig. 2A) that hold user-permitted data. Personas are extensible data structures that not only contain the data, but define behavior for how the contained data can be distributed and used. Privacy engine 220 manages the transactions associated with reading, modifying, copying and distributing persona data. In most cases a persona represents a real-world entity (e.g., a person, corporation, government agency, etc.).

Although the particular implementations shown in Fig. 2B involve commercial web sites supporting e-commerce transactions with web browser clients, the present invention is more generally useful to support a wide variety of shared devices coupled to a network. Examples of network appliances include computers, workstations, and mobile computers running web browser or other network client software. Personal digital assistants (PDA's), entertainment devices such as music and movie players may also benefit from the privacy enhancement features of the present invention. Still more generally, communication devices such as wireless and conventional wired telephones, pagers, and the like may be used to implement network appliance component 200.

Examples of shared resources include, for example, a corporate intranet can use the mechanisms in accordance with the present invention to enable access control to shared resources such as files, computer systems, inventory management systems and the like while allowing employees and the company to preserve the confidentiality of personal information. Likewise, non-commercial sites such as government information sources can use the mechanisms of the present invention to provide improved personalized services. Accordingly, although the invention is described in terms of an e-commerce type environment it is to be understood that e-commerce is only an example of the privacy-enhanced environment in accordance with the present invention.
A first type of transaction that is enabled by the present invention is a privacy enhanced commerce or exchange transaction between a client 200 and a commerce web site 210. This transaction type is privacy-enhanced by use of the persona data structure to automatically fill in web forms, maintain transaction state, and enable personalization of the web experience according to the user's preferences, interests and other information stored in the persona.

A second type of transaction is a privacy-enhanced data mining transaction between one or more commerce sites 210 that acquire raw, processed, or derived data from privacy engine 220 in a manner that abides by user-specified permissions and behavior associated with the persona. This type of transaction is privacy enhanced by virtue of a persistent association between persona data and usage permissions established by one or more managers of the persona. Examples include using the persona data for research and development, marketing and public opinion. Other examples include using the persona data for targeted offers for goods and services that fit a need indicated by the persona. Yet another use is to allow persona data to be shared with entities with which the persona may not have any other contact (e.g., cross-selling).

Referring now to FIG. 2B, client 200 implements a browser program 201 that is outfitted with a lockbox 202 and accesses a conventional cookie file 203. Lockbox 202 may be implemented as a plug-in component to a conventional browser such as Netscape Navigator or Microsoft Internet Explorer. Alternatively, lockbox 202 may be integrated with browser 201 either through application programming interfaces provided by browser 201 or more closely integrated in the form of a custom browser 201. Lockbox 202 implements a volatile data structure for holding a copy of a persona (or a portion of a persona) associated with the current user, which is described in greater detail hereinbelow. In contrast, cookie file 203 is implemented in persistent storage of the computer 107 on which client 200 is running.
Client 200 includes network components for implementing the necessary hardware and software network protocols (e.g., transmission control protocol (TCP), User Datagram Protocol (UDP), Internet protocol (IP) and the like). Browser 201 implements other protocols such as the hypertext transfer protocol (HTTP) used for communication between browser 201 and web server 211 and web server 221. In one implementation personas are represented using XML documents therefore the protocols must support transfer of XML documents. In alternative embodiments client 200 may be configured with an exposed API supporting proprietary protocols for transporting persona data structures in which case XML support may not be required. It is contemplated that browser 201 will be enabled in most instances to operate with conventional web sites as well as privacy enhanced web sites in accordance with the present invention. Alternatively, browser 201 can be configured to operate only with privacy enhanced web sites 210.

As indicated above, lockbox 202 contains a persona data structure. In practice, lockbox 202 contains a copy or instance of a persona data structure that is persistently stored and managed by privacy engine web site 220. In essence, lockbox 202 acts as a cache for the persona while browser 201 is running. It is not required that the persona copy in lockbox 202 be a copy of the entire persistent persona. During any given session a client 200 may only need to use a small portion of the persona data structure. In these cases it is contemplated that only portions of the persistent persona be copied to lockbox 202 and additional portions are loaded on demand.

To create a persona, the user provides persona data to a mechanism, entity, or person capable of translating that persona data into a conforming electronic record. In its most basic embodiment a persona can be created by submitting a completed paper or electronic form to another person or business that creates an electronic persona record. It should be understood that a persona can be created in any variety of ways to meet the needs of a particular application or environment.
In a specific example, the user directs the browser 201 to privacy engine web site 220 using conventional HTTP request/response procedure. Privacy engine web server 221 generates web pages that enable a user to access registration services within privacy applications 222. Alternatively, client 200 could conduct transactions directly with exposed APIs of the privacy applications, although this direct access method may be more difficult to implement because it does not leverage the existing Internet infrastructure.

As an alternative to a user registering directly with privacy engine web site 220 the registration process may be initiated through an interface (e.g., web page) generated by web site 210. Web site 210 includes a persona access kit (PAK) component 212 that includes methods for accessing privacy applications 222. In this manner, web site 210 can access privacy applications such as registration and portal services through its own interface while at the same time ensuring centralized storage and control of the created persona in a manner consistent with personas created by direct access to privacy engine web site 220. This feature enables the privacy services to be "co-branded" between the commerce web site 210 and the privacy engine web site 220.

Privacy engine web site 220 is itself conveniently implemented using a web server 221 that acts as an interface for accessing privacy applications 222 and persona vault 223. Although a single web server 221 is shown, it is contemplated that a plurality of web servers 221 working independently and in cooperation under a common domain would typically be used for improved throughput and load balancing. Privacy web server 221 includes storage devices 225 supporting privacy applications 222 and for storing web pages, content and the like used by web server 221. Privacy applications 222 comprise a collection of server applications, servelets, CGI scripts and the like for implementing various privacy related services. The privacy applications expose APIs that are accessible by web server 221.

Privacy engine web site 220 is also an access point for persona vault 223 which contains the persistent versions of personas. Privacy applications
222 include various vault access mechanisms (e.g., portal services, registration, login, etc.) that enable access to data within persona vault 223. The persona data held in vault 223 can be of enormous value individually to end users and collectively for data mining purposes. Accordingly, the access mechanisms are preferably implemented with a high degree of security to prevent unauthorized access. These access mechanisms include methods for authenticating the source of any access requests and verifying the access involves data that the requestor is authorized to access.

Persona vault 223 is typically implemented as a storage area network including remote storage such as disk farm 116 shown in FIG. 1. Persona vault 223 is essentially a virtual database that may use a single integrated hardware and database management platform. Alternatively, vault 223 is implemented as a plurality of geographically and/or logically diverse mass storage facilities using diverse database management systems (DBMS) to enable access.

In implementations in which the personas are relatively small data structures that are infrequently accessed, it may be desirable to implement persona vault as a directory structure accessed via a directory access mechanism. Examples include lightweight directory access protocol (LDAP) and X.500 directory protocol. In such implementations, a directory server is implemented among the privacy applications 222.

Persona vault 223 may be replicated in whole or in part to any number of sites to improve performance, reduce access latency and/or provide redundancy. This replication may include local cache systems that support only a small subset of personas. In most applications it is not critical that all copies of the persona vault 223 remain consistent at all times, hence, lazy consistency protocols can be used. However, where coherency across all copies of a persona is desired, more aggressive coherency protocols may be used. Coherency protocols may require state information to be added to each persona or persona attributed to indicate coherency state. This state information may be stored with the distributed data or within a centralized
directory structure (not shown), created within web site 220. The configuration for a particular implementation is chosen to meet the latency and size requirements of that implementation.

Upon an initial visit to privacy engine web site 220 a user is engaged by the registration service routine that aids the user in creation of a persona. The registration service routine presents a user interface such as a web form having fields and controls enabling a user to indicate personal information and associate permissions with each item of personal information. The format and scope for this registration process is very flexible so long as the user is offered the opportunity to define permissions for each item of data provided. Fig. 3 shows a logical representation of a persona 300 illustrated as a two-dimensional table structure for ease of illustration, although a persona may in practice be implemented as a multi-dimensional data structure or a single-dimension database structure (i.e., a single column in a database).

The registration process is completed by associating a user name and password with persona 300. Alternative authorization and access control mechanisms may be used instead of user name and password techniques if available. Once the registration process is complete, a persona is stored to persona vault 223 where it remains persistently. In some applications a persona may be timestamped so that if it is not used for a specified period of time (e.g., one month, six months, etc.) it will expire and be deleted or marked as invalid within persona vault 223. This is largely a "garbage collection" issue to avoid populating the persona vault resources with unused persona data structures.

In an exemplary implementation, the registration process also supplies lockbox and valet components 202 and 204 to browser 201 in a manner that integrates their functionality with the off-the-shelf browser product. Lockbox 202 may in practice be installed at any time before or after the registration process. For example, software for installing a lockbox may be provided in a mailer or as a companion to other software such as browser software. In these
cases, the lockbox may be installed before the registration process. Similarly, lockbox installation software may be provided after registration by downloading, physical media delivery, and the like.

Lockbox 202 serves as a runtime mechanism for obtaining and distributing persona data by managing authentication of itself to privacy engine web site 220 and of any web sites 201 that request persona information. As noted hereinbefore, lockbox 202 may implement a volatile data structure for holding persona information during a session. Valet 204 includes methods for reading, modifying and storing persona data by accessing privacy engine web site 220. In one embodiment valet 204 provides a scripting interface for receiving high level scripting language (e.g., JavaScript and VBScript) commands and translating those commands into calls to software components with in browser 201 and lockbox 202. In this valet 204 supports script or command line queries from web sites 210 to provide information associated with a persona directly from the browser 201.

A user can access the stored persona 300 via an HTTP request to web server 221 with the appropriate security information. Web server verifies the security information and returns a copy of the persona (or a portion of the persona) to browser 201 where it is stored in local memory. Alternatively, browser 201 sends an authorization message to privacy engine web site 220 in response to the persona request from web site 210. The authorization is authenticated by privacy engine 220. Once authenticated, privacy engine 220 waits for a request for the persona data from web site 210, authenticates that request, and supplies the requested data directly to web site 210. Alternatively, privacy engine 220 may push the persona data to web site 210 after authenticating the request from browser 201.

Preferably any time persona data is transferred across a public network or stored in persistent storage it is encrypted using available encryption techniques such as RSA, data encryption standard (DES) or the like.
Authentication is accomplished by key exchange algorithms that can be implemented to achieve any desired level of assurance.

In some implementations persona 300 is not stored persistently in client 200. In some implementations volatile memory the persona is more immune to unauthorized access by hackers than it would be in the client's persistent storage. In other implementations the persona 300 can be made as secure or more secure in persistent storage through encryption techniques. An important consideration in the selection of whether to implement volatile storage is whether the particular platform on which client 200 is implemented provides adequate security to meet the user's needs. This security includes not only encryption ability, but also analysis of unauthorized accessibility by other users either directly or through network access.

Persona maintenance and changes are implemented by privacy engine web site 220 in the preferred implementations. Alternatively, it is contemplated that valet 204 may enable routines to update, view, and/or modify contents of a persona instance within lockbox 204 and save the modified version back to persona vault 223.

Referring again to Fig. 3, a persona 300 includes a first section of persona attributes comprising core attributes 301, custom attributes 302, and a second section 303 of entity identifiers. The persona data structure 300 is readily extensible to include other sections and sets of data within those sections. Core attributes 301 include values indicating such things as name, contact preferences, date of birth, and email address in the particular example. By default, core attributes are managed by the individual identified by the core attribute values (i.e., owner ID="00000").

In some instances, such as in the case of a "child persona" described hereinbelow, the manager of core attributes may be different, or multiple managers may be designated for a given attribute. It is contemplated that the owner may be a legal entity such as a business or corporation rather than an
individual. Moreover, the core attribute values may be set to pseudonym values if so desired by the user. A defining characteristic of the core attribute set 301 is that every persona will have these attributes defined.

In contrast, custom attribute set 302 comprises an extensible set of attributes developed within a persona 300 over time. Typically a web site 210 will request information from or derive information about a user, or otherwise desire to associate some information with a particular user. This information includes, for example, purchasing preferences, store account information, demographic information, recent purchases, and the like. The present invention does not impose any restrictions on the type, purpose, or data gathering method of the data gathered by web site 210.

In this context it should be understood that web site 210 is only associating data with the persona, and so only indirectly associating the data with the user corresponding to the persona. In the past a web site might use conventional cookies to store this information on the user's machine 107. However, a cookie in practice only creates an association between the user's machine and not the user itself nor a persona 300 managed by the user.

When permitted by the user, the persona 300 can be modified to allow the information created or gathered by web site 210 to be written to persona 300 as one or more custom attributes 302. In the preferred examples a user specifies whether persona 300 can be modified and any conditions that must be satisfied before persona 300 is modified. For example, in some implementations a user may prohibit any modifications from third parties. In other implementations a user may require notification in the event of modifications from third parties. This choice might offer a high degree of privacy protection sought by the user, but would prevent web site 210 from storing any state information that would allow personalization of subsequent interaction between the user and web site 210. Alternatively, a user may allow all modification by any web site 210.
More often, the user will specify a rule or set of rules that describe who, when, and how persona 300 can be used. These rules are preferably indicated on an attribute-by-attribute basis in the opt-control preferences portion of persona 300. Alternatively, rules can be specified to arbitrary or defined groups of attributes or to all attributes. User-specified rules can specify particular web sites, individuals, or entities that are allowed to modify persona 300. Rules may also specify time periods for which modifications can be made (e.g., changes are authorized during March, 2001, but prohibited at other times). Rules may also specify how a modification is made (e.g., an attribute can be added only if it is not shared with any other web site). Moreover, a rule might specify an action that occurs upon a modification such as a notification delivered to the persona owner.

In the particular example, each rule is implemented on privacy engine web site 220 by a rules server application within privacy applications 222. Rules generally take the form of filters, triggers and constraints implemented as scripts or servlets or applications. Whenever a persona 300 is accessed through web server 221, the rules specified in the persona are applied to the access request. Hence, the persona becomes a persistent, continuously available entity of the network environment with its own unique set of state information and rules for distribution, use and modification of that state information. The persona 300 remains available and active even when the user is disconnected from the network environment. This significant feature enables the persona to exist as a proxy or agent acting on behalf of the user. For example, a web site 210 might wish to notify a persona of a sale event.

However, web site 210 only has a relationship with persona 300, and does not necessarily know the identity of the user that owns persona 300. This would be the case if, for example, the user specified the "email=" attribute as not shared to reduce junk E-mail or protect the user's identity. However, the user may specify rules that allow web site 210 to add or modify a separate attribute that holds information about the sale event. The user may be notified about the sale event from a notification event triggered by the change, or by direct perusal
of the contents of persona 300. These and other applications are made possible by persona 300 in accordance with the present invention.

Rules can be made arbitrarily complex and may be used alone or in series or parallel combination to effect complex management of persona attributes. Privacy engine web site 220 must support each rule and can update, modify and extend rules from time to time to meet user needs. The variety of rules that can be established is not restricted and is readily modified to meet the needs of a particular application.

Operation of the present invention after a persona is established with reference again to FIG. 2B. When a user logs on browser 201 retrieves the user's persona 300 from Privacy engine web site 220. To accomplish this, the user specified the user name and password associated with persona 300 in a HTTP request in a particular example. Preferably the user name and password are encrypted before transmission across any public network. Alternatively, other unique identifiers may be used. For example, the shared resource may associate a credit card number, social security number, mailing address, telephone number or the like with the persona, which may allow access to the persona. Also, the client, web site, or other entity or group of entities may obtain a transaction ID from site 220 that can be selectively enable those web sites to obtain persona data for a specified period of time for specified purposes. Persona retrieval may be required at the initiation of a session of browser 201 or deferred until a commerce web server 210 inquires about a persona.

Browser 201 sends and HTTP request to web site 210 in a conventional manner. This usually involves a resolver routine within browser 201 or its associated network protocol stack that queries one or more domain name servers (DNSs) to obtain the fully qualified IP address of web site 210. Similar address discovery protocols exists for other network architectures.
Alternatively, browser 201 may be aware of the IP address directly therefore not require the assistance of domain name services.

Privacy enhanced web site 210 receives the HTTP request and generates an HTTP response back to browser 201 to determine whether browser 201 has a lockbox 202. Web site 210 is typically configured to operate with both conventional web browsers 201 as well as browsers 201 having a lockbox. The lockbox request from web site 210 includes a unique web site identifier assigned to the web site 210 typically in the form of a unique ID number. In response to the lockbox request, browser 201 queries the persona stored in lockbox 202 to determine what data, if any, from the persona is permitted to be transmitted to web site 210.

Once the permitted data is transferred from lockbox 202, web site 210 can personalize the web site content, interface and action according to the received information. Web server 211 implements web site 210 by responding to HTTP requests with content selected from storage device 213. In a typical application web server 211 delivers static or dynamic HTML pages to browser 201 and/or references to other Internet resources that have content. In a particular application the content is selected based on criteria supplied in the persona.

Web server 211 can also use the persona information to aide in transaction processing either by directly using data included in the persona (e.g., credit card information and shipping address) or by using the persona information to extract this transaction-related information from its own local database. Using the persona information directly had an advantage of ensuring the data is fresh as it is under continuous control of the user whereas stored data may have become incorrect since the last access. Significantly, the web site is able to use persona information that was not created by the web site itself. Unlike conventional cookie mechanisms, the persona includes attributes
generated by the user and by third parties in addition to information previously stored by the web site itself.

Web site 210 is enabled to interact with personas by a persona access kit (PAK) 212 that is added on or integrated with conventional web server software 211. PAK 212 may take on one of a variety of forms depending on the needs of web site 210. Basic functionality enables PAK 212 to request persona information from browser 201 and transfer the returned persona information in a form that can be used by web server 211. Other functionality may include an ability to create or modify attributes within the received persona through interaction with browser 201 or directly through interaction with privacy engine web site 220. Still other functionality may enable the PAK 212 to extract information directly from privacy engine web site 220 by accessing privacy applications 222, subject to permissions established in the persona.

Each PAK instance is assigned a globally unique ID on behalf of web site 210. The globally unique ID is used by browser 201 and privacy engine web site 220 to identify the particular web site that is requesting access to a persona 300. Although the web site's domain name is a unique identifier, this domain name does not authenticate that the web site is PAK enabled (i.e., privacy enhanced). Also, domain names can be spoofed or counterfeited by skilled hackers. By using a globally unique ID the web site is readily identified as a privacy enhanced site and the permissions granted to that site can be verified. To prevent unauthorized access, the web site's ID is encrypted in any communication across a public network.

The persona data structure can be expressed in a number of ways including representation as programming constructs (e.g., Java, C++ classes and the like) database objects and entities, structured documents (e.g., XML, HTML, UML), and the like. Any mechanism suitable for storing and transporting the persona data and relationships between persona components is a suitable equivalent. FIG. 4 and FIG. 5 illustrate an implementation in which extensible markup language (XML) format data structures are used to
implement personas 300. The actual persistent format of personas 300 in persona vault 223 is determined by the hardware and database management software used to implement vault 223. The XML format structures shown in FIG. 4 and Fig. 5 are useful for transferring persona information between entities such as vault 223 and client 201 and/or web site 210. XML is useful in the practice of the present invention because it is capable of representing hierarchical relationships between data, is readily extensible, largely platform independent, and is supported by a wide range of existing development tools.

Fig. 4 shows an exemplary document type definition (DTD) that defines a valid structure of a persona 300. Tools that read and write XML personas can use the DTD to create valid structures and to determine whether a received structure is valid. This validation is accomplished by a validating parser, which reads the DTD from privacy engine web site 220 and ensures the XML of the received persona is properly composed.

DTD 400 includes an entities section and an attributes section. The entities section defines an "entity definition" structure for containing identifications of web sites 210. Each entity definition comprises a name and an ID. The name is a preferably a human readable name such as a corporation name, vendor name, or the like (e.g., "General Motors" or "IBM"). The ID is a globally unique identifies assigned to the entity such as the globally unique ID assigned to PAK 212 of web site 210.

The attributes section comprises a series of attribute definitions called ATTR in FIG. 4. Each attribute comprises a name:value pair as well as information describing the manager of the attribute and the user-specified opt-preference information. The preference information indicates which vendors have access to the attribute value. The "USAGE" field in Fig. 4 is a structure that enables the specification of rules to be applied by rule server software within privacy applications 222 that specify specific reasons that access is permitted. The "MANAGER" information contains data about what entity owns
the attribute as well as the data that determines what other entities have access to the field.

An exemplary persona definition 500 in compliance with DTD 400 is shown in FIG. 5. The persona definition is a structured document that follows the rules defined in the DTD. The persona may be transmitted between the persona vault 223 and vault clients 201, or between any set of cooperating programs. Persona definition 500 includes a header that defines the document as an XML document based on the Persona DTD 400 for its structure. A validating parser will access the DTD 400 from the location "http://tech.privaseek.com/DTD/persona.dtd" in order to parse and validate the document structure. Line 2-line 6 of persona 500 include an exclamation point "!" indicating comment text. The "PERSONA" tag indicates the beginning of the persona definition per-se.

The entity section 502 defines an entity having a privacy enhanced network resource such as website 210. Each entity definition comprises an ID used to identify the merchant and a user-friendly name used to display the merchant information in human readable interfaces. Attribute section 503 contains definitions and values of all attributes that were requested by the client 201 and present in the persona. In the example of FIG. 5, the first attribute describes the first name of the user associated with the persona. The attribute name is "User.Name.First" and the value assigned is "Greg". The next statement ("GRANTED ID='ALL'") denotes that the user has granted permissions to all entities that request access to this attribute. The granted permissions ("USAGE='ALL'") indicate that the user is permitting any to use the attribute for any reason. "AUTHREQ='N'" indicates that no runtime authorization required. Significantly, these permissions are applied only to the attribute named "User.Name.First"—all other permissions are denoted in separately defined attributes.

The "Manager=" clause of the attribute is set to a value indicating entity 00000, which by way of reference to entities section 501 indicates the manager...
is an entity named "Privaseek". Privaseek.com, the assignee of the present invention, is the operator of privacy engine web site 220 in the particular examples herein, and so is the default attribute manager. The designated manager entity is responsible for allowing the user to create and maintain the value. In addition, the manager has certain rights with regard to whom the value of the attribute is released to. In the example of Fig. 5, the manager has specified that the attribute value is shared and accessible to any entity for any use, subject to the permissions specified in the "GRANTED" clause described above.

The concept multiple entity control over an attribute is important to recognize. In the battle between privacy and personalization a major stumbling block has been a tendency to designate data as owned and controlled by a single entity. The present invention does not attempt to resolve these issues by dogmatic declarations of data ownership. Instead, a persona enables multiple entities to affect use of the attribute value. Like the people and organizations that a persona serves, a persona can be controlled by the user, the user's employer, the user's parent, as well as an interested third party such as a web site 210 or a governmental entity. These ownership or managerial interests are hierarchically ordered so that the rules server in privacy applications 222 can arbitrate amongst the interests to determine how an attribute is distributed.

In the preferred implementations described herein, a simple arbitration rule that offers the most privacy protection is enforced. Specifically, data is not distributed when any entity has expressed an interest (via an appropriate value setting in a persona) that would prohibit the attribute's distribution. Other arbitration rules might be implemented, however, including voting algorithms to vote amongst interested entities where the votes are distributed according to relative interest. Such as system can still give the user ultimate control of the distribution while enabling inferior interest holders to determine distribution behavior when the user has not designated a preference.
Another attribute definition 503 in persona 500 illustrates a persona that is managed by an interested third party such as an entity named "Amazon.com". The named entity corresponds to a network resource such as web site 210. The network resource is a registered resource meaning that it has an assigned global ID and is defined in the Entities section of the persona. It should be understood, however, that although the present invention is described in terms of web sites, a network resource can be any type of network resource including file systems, email systems, a client 201, and the like. In this second case the attribute is named "Amazon.Purchase.LastTitle" and its value indicates that the most recently purchased book was "The Cluetrain Manifesto".

The user granted permissions only extend to Amazon.com and the user has opted to permit only uses specified as "01" and "02". The specified uses correspond to rules recognized by the rules server software. For example, usage rule "01" might allow the attribute to be released to Amazon.com for statistical modeling purposes while usage rule "02" might allow the same attribute to be released so that Amazon.com may determine if any books by the same authors have been published. The definition of rules is virtually unlimited as described hereinbefore. Because the rules are only identified within a persona and not defined within the persona, the persona is compact, portable to a variety of rules server implementations, and can stand alone as an independent entity or agent representing the users desired usage permissions. In this sense the persona becomes an autonomous agent representing the user.

In the Amazon.com.purchase.lasttitle attribute the designated manager is the entity Amazon.com. In the example of Fig. 5, the manager has specified that entities corresponding to General Motors, Proctor and Gamble, and IBM have access to the entity (subject to the user permissions specified in the GRANTED clause). In addition, IBM's access to the attribute expires at 10 AM mountain standard time on January 31, 2001.
The final attribute defined in FIG. 5 is an example of a private attribute named "Amazon.Purchase.PurchaseDate". This attribute has a value indicating the last purchase date, and user granted permissions extend only to Amazon.com. The permission grant extends to all uses of the attribute. Amazon.com is defined as the Manager, but because no sharing is defined the attribute is only allowed to be used by Amazon.com. The lack of defined sharing distinguishes this attribute as private. Hence, any request for this attribute by an entity other than the manager will not return the attribute value.

Fig. 6 illustrates a special-purpose a persona called a "child-persona". A useful feature for consumers to feature that allows them to protect the personal information of their minor children. In some cases it is useful to allow a Web site to 210 to collect limited information about a minor for customization of the experiences and for other reasons. However, the parent must have ultimate control over the information default. In addition, the children may have the ability to customize some information about themselves (e.g., favorite hobbies, colors, etc.) the parent must have ultimate authority to override those customizations.

A similar situation in exists within a corporate structure, school environment, or other business or government entity allowing employee Web access. It may be important to an employer to control the company's private information that may be inadvertently disclosed by employee Web use. Moreover, an employer might wish to prevent disclosure of the company's identity while employee uses the Internet for personal purposes. The child persona model handles of the use and similar situations with a little modification.

The child persona is based on an idea that there is sensitive information, i.e. information that can identify the child or otherwise put the child in potential harm. Furthermore, whether information is sensitive or not often depends on the context. For example, providing a first name and last name is not necessarily a problem, but combining it with any e-mail address may be.
Because it's difficult or impossible to know with certainty the implications of certain combinations of data, it should be possible to employ an extremely conservative model of information delivery.

As compared to the specific examples given herein, a child persona may include any number of modifications in the content and relationships between that content to provide a desired level of protection and control over the child persona in a particular environment. Important, but not exclusive, requirements of a child persona protection include:

- Ability to specify only limited amounts of information;
- Ability to participate in Web interactions requiring the use of personal information;
- Ability to hold or defer all Web transactions pending approval by a parent;
- Ability to defer changes pending approval by a parent.

Given the above requirements, a child persona is readily incorporated into the above-described persona infrastructure. Essentially a child persona follows a model in which a parent is assigned a digital identification. A parent can create a child persona to be used by their child. The child persona contains the information specified initially by the parent. The parent persona's digital ID is noted in the child persona. The child can use the persona to access Internet resources and interact with persona-enabled sites. The parent can specify the ability for child to use a credit card number owned by the parent persona as well as a preset spending limit. The parent can specify the required privacy preferences associated with the child persona. The child has the ability to modify the persona, with changes affected after parental acceptance. Changes made to the child persona are e-mailed to the parent's e-mail address of record. Alternatively, any available means of notification may be used. To accept the changes, the parent must digitally sign an affirmative reply to the change request with their digital ID. To actively canceled changes, the parent
must digitally sign a negative reply to the change request with their digital ID. Changes will be canceled automatically if the parent does not respond with a sign affirmative reply with any given time frame. These act to the use and behaviors are readily implemented in privacy applications 222 shown in Fig. 2B. These policies are a matter of design choice and other policies may be implemented in a particular application. Moreover, the specific example above relies on the digital ID of the parent to authenticate parental control, however, other means of authentication and control may be available and should be considered in a particular implementation of the present invention.

With these behaviors, the child persona can be used in much the same manner as any other persona. In order to work correctly, the child persona should only operate on privacy-enhanced Web sites. Otherwise no accounting is available for the use of the data. In other words, browser 2001 is configured such that when a child persona is active in lockbox 202 it can only display content from Web sites that are PAK-enabled.

As noted hereinbefore, a second class of privacy-enhanced transactions enabled by the present invention include "data mining" transactions. The extensible and flexible nature of personas make the persona a valuable spot for collecting data about that persona's excursions and transactions on the internet. A mature persona will be populated with attributes from a variety of web sites as well as attributes about the real-world entity associated with the persona. Collectively, personas can be "mined" to for research and development uses, target marketing, and cross-selling among other uses.

Data mining type uses need to be carefully managed so that they benefit consumers without violating the consumer's desire for privacy. The ad-hoc manner in which data mining is being applied in many data environments leads to mistrust and misuse of information. Because the persona data structure implements user-specified distribution behavior, it is advantageously employed
to enable data mining in a manner that does not violate consumer desires for privacy.

Referring back to FIG. 2B, a PAK 212 can be configured to access persona vault 223 without involving a client 200 to obtain collections of persona data. Significantly, a PAK 212 can only access user-permitted data even though the user is not directly involved in the data mining transaction. A request for persona data must be accompanied by a valid ID indicating who the requestor is as well as an indication of the purpose for which the data will be used. The ID and usage statements in the request are validated against the usage rules specified in the persona before persona data is distributed.

In operation, a web site 210 makes a request for persona data to privacy engine 220 either on-line or off-line. The request will typically indicate filters to be applied. For example, a web site 210 may request 10,000 personas corresponding to consumers aged 25-35 that have purchased a product through any web site in the last 30 days. In practice the request will typically identify the kind of data it wants returned from the personas such as first name, last name, email address and the like.

Privacy engine 220 then queries persona vault 223 to identify the personas meeting the criteria. The rules server is applied to the attributes of the identified persona to restrict any attributes that are not permitted to be distributed for the stated use. The package of data may then be formatted for transmission to the requesting web site. This formatting typically involves encryption to prevent plaintext transmission of persona data.

Essentially, privacy engine 220 provides a repository for personal data and software applications that implement methods for accessing and manipulating the personal data. The repository can be implemented as a centralized network-connected entity for responding to requests from other network-connected entities and servicing those requests. Alternatively, privacy engine can be implemented in a distributed fashion with a plurality of replicated
privacy server applications and/or a replicated persona vault 223 for storing and manipulating the personal data in a distributed fashion. Replication may provide advantages through geographic/logical distribution and redundancy. Geographic distribution allow provides lower latency response in some applications. Redundancy can prevent or inhibit bottlenecks that may otherwise occur when many network connected entities attempt to communication with privacy engine 220. Redundancy also improves availability of the system in that degradation or failure of one redundant copy can be temporarily overcome by the other redundant copy or copies. Appropriate coherency mechanisms (not shown) are implemented to maintain a desired level of consistency across these distributed resources.

In addition to replicating the data storage portions of privacy engine 220, in some cases the application server portions may be replicated and/or distributed in whole or in part. One example described hereinbefore is the implementation of rules server within client software, for example. In many environments it may reduce latency to clients by implementing privacy engine 220 as a plurality of web servers (or other network server) such as 220a and 220b shown in Fig. 6. Any number of privacy engines can be distributed throughout a geographic area. Each server would run a complete set or subset of privacy applications. One or more routing servers 230 can direct clients 201 to an appropriate server 220a or 220b to accomplish a particular task using conventional redirection mechanisms available in HTTP. Alternatively, appliances 220 may have a fixed relationship with a selected privacy engine 220a or 220b in which case router 230 may not be required.

In operation, privacy engine 220 responds to both network appliances and network resources as shown in Fig. 2A. In a first type of transaction a network appliance requests a persona from privacy engine 220 using an HTTP request packet. After authentication and validation of the request privacy engine 220 generates an HTTP response including the persona or requested portion thereof. The HTTP response may include an XML expression of the
persona in the payload. Alternatively, the persona may be set by setting "cookies" in the appliance 200 using HTTP set-cookie header. Subsequently the network appliance 200 can use the persona data to customize its own operation and/or distribute the persona data (according to rules within the persona) to enable other network entities and applications to customize and/or personalize their performance.

In another mode of operation privacy engine 220 negotiates a transaction ID with a network connected entity such as appliance 200 and/or resource 210. Persona data can be served on demand to any network entity holding the transaction ID. In this mode the actual persona data may also be distributed as a structured document (e.g., XML) embedded in the HTTP response or as cookies.

In yet another mode of operation an appliance 200 authorizes privacy engine 220 to deliver selected profile data to a specified network resource. In response, privacy engine authenticates the request, validates that the request is directed to entities that have permission to receive the data, and that the requested data will be used for permitted uses. Once authenticated and validated, privacy engine 220 pushes the persona data out to the targeted resource. This can be done, for example, by causing privacy engine 220 to generate an HTTP request directed to the target resource 210 and including cookies in the HTTP request. The included cookies express the persona data. The included cookies must be generated by privacy engine 220 so as to have a domain specified that is the same as the domain of the target resource 210. Many exemplary network connected resources such as web servers have built-in mechanisms for handling information transmitted by cookies.

In this manner, the persona data structure in accordance with the present invention expresses the personal data along with the distribution and usage preferences specified by the user. The persona remains continuously available for transactions involving the user as well as transactions between network connected resources 210 and privacy engine 220 that do not involve
the user. The persona management tools implemented by privacy engine 220 enable the persona attributes and distribution preferences to be modified both by users and third parties. Because the persona continuously enforces the distribution preferences stated in the persona, it remains a continuously vigilant protective mechanism for controlling the distribution of private data.

Although the invention has been described and illustrated with a certain degree of particularity, it is understood that the present disclosure has been made only by way of example, and that numerous changes in the combination and arrangement of parts can be resorted to by those skilled in the art without departing from the spirit and scope of the invention, as hereinafter claimed.
WE CLAIM:

1. A persona data structure for identifying an entity in a network environment comprising:
   a plurality of (hierarchically ordered) attributes (persistently stored only in a data vault having a secure API);
   a manager designation associated with each attribute, the manager designation identifying an entity that is enabled to set permissions for the attributes;
   a permission vector for each attribute, the permission vector indicating opt-control preferences set by the attribute's associated manager.

2. The persona data structure of claim 1 wherein attributes within a given hierarchy tree have a plurality of manager designations.

3. The persona data structure of claim 1 wherein the data structure is does not include explicit or implicit relationship data to any other persona data structure.

4. The persona data structure of claim 1 wherein the manager designation is implemented as a hierarchical management structure such that a first designated manager is superior to, inferior to, and/or a peer with at least one other designated manager.

5. The persona data structure of claim 1 wherein the persona is a child persona and the manager designation is a parent persona data structure.

6. The persona data structure of claim 1 wherein any change to an attribute or the permission vector associated with an attribute is reported to the manager designated for the attribute.

7. The persona data structure of claim 2 wherein any change to an attribute or the permission vector associated with an attribute is reported to each manager designated for the attribute.
8. The persona data structure of claim 1 wherein each persona includes an attribute identifying a name and email address for a person represented by the persona.

9. The persona data structure of claim 1 wherein at least one attribute is associated with multiple managers and each associated manager has an arbitral ability to control the permissions for the attribute.

10. A system for creating a data structure holding privacy-controlled data comprising:
    a network appliance having a user interface for interacting with a user,
    and a connection to a network;
    means for enabling the user to specify information attributes;
    means for enabling the user to associate with each information attribute a privacy control vector; and
    means for storing the specified attributes and associated privacy control vector in a data storage device.

11. A system for managing use of privacy controlled information in a data communications network comprising:
    a network appliance including mechanisms for communication with the network;
    a data storage area within the network appliance for storing a downloadable persona data structure, wherein the persona data structure includes privacy controlled information;
    a privacy engine running on the client system, the privacy engine being responsive to the persona data structure to selectively communicate the private information with third parties; and
    a persona vault coupled to the communications network through a secure application programming interface (API), the persona vault providing persistent storage for the persona data structure.
12. The system of claim 11 wherein the persona engine is configured to access the persona vault and retrieve the persona into the client systems volatile data storage area.

13. The system of claim 11 wherein the persona engine is configured to allow persistent storage of the persona only in the persona vault.

14. The system of claim 11 wherein the persona comprises a plurality of attributes where each attribute includes a permission vector and a designated owner.

15. The system of claim 11 further comprising a privacy enabled server coupled to the network, the server configured to provide services using the private information.

16. The system of claim 11 wherein the persona vault comprises a virtual database.

17. The system of claim 11 wherein the persona vault comprises a replicated database.

18. The system of claim 11 wherein the persona vault includes a cache data structure for temporary storage of personas, the cache data structure operative to reduce latency associated with accessing a persona.
This is an example XML representation of a Persona. It illustrates the basic principles and attributes of a Persona.

```
<?xml version="1.0"?>
<PERSONA VERSION="1.0">
  <ENTITIES>
    <ENTITY NAME="PrivaSeek" ID="00000"/>
    <ENTITY NAME="General Motors" ID="02361"/>
    <ENTITY NAME="Amazon.com" ID="00024"/>
    <ENTITY NAME="Barnes and Noble" ID="00983"/>
    <ENTITY NAME="Proctor and Gamble" ID="14332"/>
    <ENTITY NAME="IBM" ID="00019"/>
  </ENTITIES>
  <ATTRIBUTES>
    <ATTR NAME="UserName.First" VALUE="Greg">
      <GRANTED ID="ALL" USAGE="ALL" AUTHREQ="N"/>
      <MANAGER ID="00000">
        <SHARED>
          <GRANTED ID="ALL" USAGE="ALL"/>
        </SHARED>
      </MANAGER>
    </ATTR>
    <ATTR NAME="Amazon.Purchase.LastTitle" VALUE="The Cluetrain Manifesto">
      <GRANTED ID="00024" USAGE="ALL"/>
      <MANAGER ID="00024">
        <SHARED>
          <GRANTED ID="02361" USAGE="01, 02"/>
          <GRANTED ID="14332" USAGE="01, 02"/>
          <GRANTED ID="00019" USAGE="01, 02"/>
        </SHARED>
      </MANAGER>
    </ATTR>
    <ATTR NAME="Amazon. Purchase. PurchaseDate" VALUE="5/4/1999">
      <GRANTED ID="ALL" USAGE="ALL"/>
      <MANAGER ID="00024"/>
    </ATTR>
  </ATTRIBUTES>
</PERSONA>
```
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 17/60
US CL : 709/203, 217; 705/27, 14
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/203, 217; 705/27, 14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 5,913,030 A (LOTSPIECH et al) 15 June 1999, cols 3-6.</td>
<td>1-10</td>
</tr>
<tr>
<td>A</td>
<td>US 5,710,884 A (DEDRICK) 20 January 1998.</td>
<td>1-18</td>
</tr>
<tr>
<td>A</td>
<td>US 5,724,521 A (DEDRICK) 03 March 1998.</td>
<td>1-18</td>
</tr>
<tr>
<td>A</td>
<td>US 5,724,567 A (ROSE et al) 03 March 1998.</td>
<td>1-18</td>
</tr>
<tr>
<td>A</td>
<td>US 5,740,549 A (REILLY et al) 14 April 1998.</td>
<td>1-18</td>
</tr>
</tbody>
</table>

☐ Further documents are listed in the continuation of Box C.
☐ See patent family annex.

* Special categories of cited documents:
- "A": document defining the general state of the art which is not considered to be of particular relevance
- "E": earlier document published on or after the international filing date
- "L": document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O": document referring to an oral disclosure, use, exhibition or other means
- "P": document published prior to the international filing date but later than the priority date claimed
- "T": later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X": document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y": document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&": document member of the same patent family

Date of the actual completion of the international search: 16 MAY 2001
Date of mailing of the international search report: 14 JUN 2001

Name and mailing address of the ISA/US Commissioner of Patents and Trademarks:
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer: [Signature]
Telephone No. (703) 305-2000

Form PCT/ISA/210 (second sheet) (July 1998)*