

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
2 May 2008 (02.05.2008)

PCT

(10) International Publication Number  
**WO 2008/049234 A1**

(51) International Patent Classification:  
**G06F 21/00** (2006.01)

(21) International Application Number:  
PCT/CA2007/001918

(22) International Filing Date: 26 October 2007 (26.10.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/854,990 27 October 2006 (27.10.2006) US  
60/855,011 27 October 2006 (27.10.2006) US  
60/855,133 27 October 2006 (27.10.2006) US

(71) Applicant (for all designated States except US): **XYSTAR TECHNOLOGIES, INC.** [CA/CA]; 662 King Street West, Suite 105, Toronto, Ontario M5V 1M7 (CA).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **CRAIG, Terrance Michael** [CA/CA]; c/o Xystar Technologies, Inc., 662 King Street West, Suite 105, Toronto, Ontario M5V 1M7 (CA).

(74) Agents: **RUSTON, David A.** et al.; Sim & McBurney, 330 University Avenue 6th Floor, Toronto, Ontario M5G 1R7 (CA).

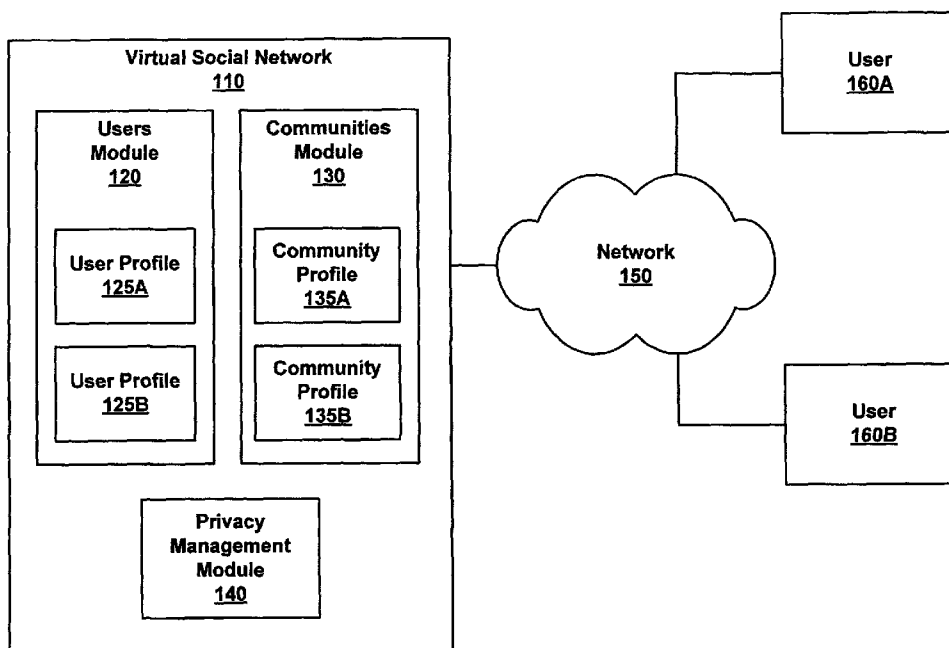
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN,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

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

(54) Title: SELECTIVE PRIVACY MANAGEMENT IN VIRTUAL SOCIAL NETWORKS



(57) Abstract: Systems and methods for privacy management of user content in virtual social networks are provided. A user of the virtual social network can designate user preferences to be associated with the content provided by the user. The user preference authorizes one or more individuals to access some or all of the user's content in the virtual social network. In various embodiments of the present invention, the user may authorize specific groups of individuals by designating a set permission associated with each group.

WO 2008/049234 A1

## SELECTIVE PRIVACY MANAGEMENT IN VIRTUAL SOCIAL NETWORKS

### BACKGROUND

#### Field of the Invention

[0001] The present invention relates generally to the field of virtual social networks. More specifically, the present invention relates to privacy management in virtual social networks.

#### Description of Related Art

[0002] Various virtual social networks allow a user to connect and interact with other individuals. Each user of a social network may choose to interact with certain other users of the virtual social network and form connections with those users. Forming a connection with an individual may consist simply of designating the individual as a friend, a contact, or some other designation. In some virtual social networks, the designation can be reciprocated. For example, two users may designate each other as a friend. The virtual social network allows for each user to form, organize, and manage all such connections.

[0003] One way for users to meet and otherwise interact is through a community in the virtual social network. Created by an administrator, an individual user, or the like, a community represents an aggregation of users within the virtual social network who typically share something in common. A community is, therefore, generally directed toward a particular subject matter. Users with an interest in the subject matter may join the community and interact with other users with a similar interest. The subject matter may be, for example, social, hobby-related, fan-related, or business-related. A user may choose to create or join various communities corresponding with any of that user's interests.

[0004] A community can allow for various activities, such as posting articles, blogs, photos, or video. Access to the content posted by a user may be given to the

general public or can be restricted, as determined by the user, by rules of the community, and/or by rules of the virtual social network. Some virtual social networks allow the user to restrict access to the content so that only individuals associated or connected with the user may view the content posted by the user. For example, user may only allow the user's friends to view the content in the virtual social network that is associated with the user.

## SUMMARY OF THE INVENTION

[0005] The present invention provides for systems and methods of selective privacy management in virtual social networks. Access to content provided by a user is controlled by preferences designated by that user. A user preference may authorize one or more individuals to access some or all of the content. In various embodiments of the present invention, a user preference may also authorize a specific group of individuals, or a friend set to view the associated content.

[0006] Embodiments of the present invention provide for methods of managing the privacy of user content in a virtual social network. An exemplary method comprises receiving content specified by a first user of the social network and associating a user preference with the content, the user preference limiting who is authorized to access the user content. This method further comprises receiving a request from a second user for access to the user content and determining from the user preference whether the second user is authorized to access the user content. The present invention also provides a computer-readable storage medium having stored thereupon executable computing instructions for performing the method just described.

[0007] The present invention also provides systems for managing the privacy of user content in a virtual social network. An exemplary system comprises an input module configured to receive content specified by a first user of the social network, a database configured to store a user preference associated with the content, the user preference limiting who is authorized to access the user content, and an access control module configured to determine from the user preference whether a second user is authorized to access the user content. Some embodiments of the present invention further include a friend set database for storing information concerning groups of individuals in the virtual social network. Friend sets allow the user to manage and designate groups of individuals.

**BRIEF DESCRIPTION OF THE DRAWINGS**

[0008] FIG. 1 is an illustration of a web-based implementation of a virtual social network, according to an exemplary embodiment.

[0009] FIG. 2 is an illustration of a user profile in a virtual social network, according to an exemplary embodiment.

[0010] FIG. 3 is an illustration of a community profile in a virtual social network, according to an exemplary embodiment.

[0011] FIG. 4 is an illustration of a system for selectively managing the privacy of user content in a virtual social network, according to an exemplary embodiment.

[0012] FIG. 5 is a flowchart illustrating a method for selectively managing the privacy of user content in a virtual social network, according to an exemplary embodiment.

## DETAILED DESCRIPTION

[0013] The present invention includes systems and methods for selectively managing the privacy of content made available in virtual social networks. A user designates a preference to control access to content provided by the user. A user preference authorizes one or more individuals to selectively access some or all of the content. This user preference is associated with the content, and access to that content is then restricted to those individuals designated by the user. The user can choose to make public or selectively restrict access to any content that the user posts or creates a link to in the virtual social network. In various embodiments of the present invention, the user may also designate a specific group of individuals, or a friend set, as authorized to view the particular content.

[0014] FIG. 1 is an illustration of a web-based implementation of a virtual social network 110, according to an exemplary embodiment. The virtual social network 110, comprising users module 120, communities module 130, and privacy management module 140, is accessible to exemplary users 160A and 160B through a network 150, such as the Internet or an intranet. Users 160A and 160B each have a respective user profile 125A and 125B, managed by users module 120. Communities module 130 manages profiles for various communities, such as community profiles 135A and 135B for exemplary communities A and B (not pictured).

[0015] A module (or application), as referenced herein, should be generally understood to be a collection of routines that perform various system-level functions and may be dynamically loaded and unloaded by hardware and device drivers as required. The modular software components described herein may also be incorporated as part of a larger software platform or integrated as part of an application specific component.

[0016] Virtual social network 110 is configured to allow a user to create, manage, and maintain that user's collection of relationships with other individuals in a virtual environment. Virtual social network 110 allows the user to encounter, interact with, and connect with new acquaintances that also use virtual social network 110. Thus, virtual social network 110 may be used to create new

connections, thereby expanding the user's collection of relationships. For example, the user may also join one or more communities in the virtual social network and form connections with the fellow members of such communities. The user may also use virtual social network 110 to track, manage, and maintain existing relationships with individuals already known to the user. Virtual social network 110 includes various modules which provide ways for users to manage and interact with individuals with whom they are connected.

[0017] Users module 120 stores and manages information concerning the users of virtual social network 110. Information concerning each user may be organized, stored, and managed by users through their respective user profiles. For example, information concerning exemplary users 160A and 160B may be stored in user profile 125A and user profile 125B, respectively. Such information may include information entered by the user, such as personal information, personal descriptions, and interests. In some embodiments of the present invention, a user profile may further include information about the various activities and interactions involving the user within the virtual social network 110. Further, each user profile may include various modules which allow for the management of all of the information concerning the user within virtual social network 110.

[0018] Communities module 130 manages and stores information concerning communities in virtual social network 110. Communities may be directed toward a variety of topics, ranging from broad topics to very specialized topics. Just as topics may be related or overlap, a community concerning cars, for example, may have sub-communities concerning racecars, antique cars, car maintenance, etc. Information concerning exemplary communities A and B may be stored in community profile 135A and community profile 135B, respectively, within communities module 130.

[0019] In various embodiments of the present invention, communities module 130 allows for a user or a social network administrator to create, populate, and manage a community. Communities may be populated in a variety of ways. For example, members may be added by the community creator upon creation, or individuals may be allowed to join independently over time. Alternatively, a community may be cross-populated with members of other communities. Cross-

population of communities is further discussed in U.S. patent application 60/854,990. In some embodiments of the present invention, the community creator can restrict the membership of the community by requiring prospective members to obtain permission, invitations, or passwords from the community creator or moderator.

[0020] The user of virtual social network 110 may post content or post a link to content, which may include written, artistic, photographic, and various other types of content. Privacy management module 140 manages access to all of the content provided by the user based on preferences established by that user. A preference is a designation concerning the individual or individuals authorized to access that user content. User preferences may include default preferences to be associated with content in the absence of any specific designation to the contrary. A user can express a preference that a posted content be accessible by the public, private to the user, or restricted to one or more individuals. Described in further detail below, privacy management module 140 allows for the selective management of user content based on these user preferences. If the user posted the content to a community, access to the content may be further constrained by community rules, also enforced by privacy management module 140.

[0021] FIG. 2 is an illustration of a user profile in a virtual social network 110 (FIG. 1), according to an exemplary embodiment. User profile 125A allows User 160A to manage information and interactions within virtual social network 110. User profile 125A may include various activity modules 210A-210F, personal friend sets 220, personal messages module 230, personal profiles module 240, and the like. In various embodiments of the present invention, access to the information managed by each component can be controlled by privacy management module 140.

[0022] Activity modules 210A-210F allow for the user to interact with other users of virtual social network 110. As illustrated in FIG. 2, these exemplary modules may include articles 210A, blogs 210B, events 210C, media 210D, message board 210E, polls 210F, and the like. Users may wish to write articles, blog entries, etc., and post them to a personal page, a community page, or the like, using one of the activity modules 210A-210F.

[0023] Interaction with other individuals occurs when other users of virtual social network 110 view, listen to, and/or otherwise interact with the content provided by the user. Through privacy management module 140, the user can restrict such interaction so that it occurs only with specific other individuals. By designating a user preference to be associated with the content posted by the user, the user is able to manage who may and who may not access that content. In various embodiments of the present invention, the user can further restrict interaction by only allowing certain individuals to post comments, feedback, and otherwise respond to the content posted by the user.

[0024] The individuals in virtual social network 110 that are connected to a user may be referred to as friends of that user, and a group of those individuals may be referred to as a friend set. A user may create and populate a friend set with one or more individuals designated by the user. Examples of friend sets may include "Family" for family members, "Colleagues" for professional contacts, "Cars" for fellow car enthusiasts, "Basketball fans" for fellow sports fans, "Racing Community" for fellow members of a racing community in virtual social network 110, etc. Grouping friends into friend sets allows the user to simplify the management of his relationships. For example, the user may wish to manage every family member in a similar manner. Rather than managing each family member individually, the user may simply create a friend set for family members. Actions involving a friend set would involve each member of the friend set. A friend set is personal to the user, and information concerning friend sets may only be accessed by other individuals if the user allows.

[0025] Information concerning user 160A's friend sets may be managed using the personal friend set module 220 associated with user 160A profile 125A. Such information may include names, member lists, and various settings for each friend set. For example, the user may create a friend set, give the friend set a name, populate the friend set with designated individuals, and edit various settings associated with the friend set. These settings may include user preferences concerning access privileges to the various activities and content associated with the user. User preferences concerning default access privileges of friend sets may be

referred to as set permissions. Personal friend set module 220 also allows for the editing of friend sets. Editing may include adding members, removing members, renaming the friend set, deleting the friend set, changing various settings (e.g., permissions) associated with the friend set, and so forth. A user may authorize a friend set for access to user content by, for example, designating a default set permission associated with the friend set or by specifically designating the friend set when posting content.

[0026] Users may also send and receive personal messages from other individuals in virtual social network 110. These messages may be managed by personal messages module 230. In various embodiments, the types of messages managed by personal message module 230 may include, for example, emails, instant messages, text messages, private messages, and various content and news feeds subscribed by the user. These messages may only be accessed by the users to and from whom the messages were sent in some embodiments.

[0027] A user can have one or more personal profiles, managed by the user using personal profiles module 240. The user may wish to customize one or more personal profiles in order to convey different information to different individuals or groups associated with the user. Specific personal profiles may be tailored for each community of which the user is a member. A user who has joined a car enthusiast community, for example, may wish to create a personal profile, specifically for use in that community, detailing information concerning the user's cars and car-related interests.

[0028] Further, each personal profile may be associated with different settings, including user preferences. The user can limit access to a car-oriented personal profile so that it may be accessed and viewed only by specific friends, specific friend sets, members of specific communities, or any combination of the foregoing. For example, a user may designate that the personal profile tailored for a car community may be accessed only by members of that community. A user may create a public personal profile, a personal profile accessible only to family members, a personal profile accessible only to work colleagues, and various other personal profiles, each with its own settings concerning access. The user may also wish to use

the same profile in various communities. A personal profile may be portable and accessed through various communities. Access to a personal profile posted in certain communities, however, may be further constrained by the rules of the particular community.

[0029] FIG. 3 is an illustration of a community profile in a virtual social network 110 (FIG. 1), according to an exemplary embodiment. The modules 310-340 are analogous to the modules 210-240, respectively, discussed with respect to FIG. 2. In communities, however, the information and interactions may be managed by a community creator, moderator, the members, etc. Modules 310-340 include common member elements and may be used by any member to interact with other community members. For example, the friend sets module 320 in a car community may define friend sets by interest in different types of cars or car-related topics. Any member wishing to address other members with a specific interest may post content and establish access privileges using the applicable friend set.

[0030] Within each community, members may interact in various ways, including interaction through activity modules 310A-F. These activity modules may be directed, for example, to posting and responding to articles/news listings 310A, blogs 310B, event listings 310C, photo/video 310D, messages 310E, and polls 310F. In some embodiments, any community member can contribute content to any of the activity modules 310A-F. Content may also be provided to community members through the various channels described in U.S. patent application 60/855,133. As with the content discussed with respect to the module associated with the user 210A-210F, a user providing content may selectively determine who may access that content.

[0031] FIG. 4 is an illustration of a system for selectively managing the privacy of user content in a virtual social network 110 (FIG. 1), according to an exemplary embodiment. Privacy management module 140 may include input/output module 410, authentication module 420, friend set database 430, preferences database 440, access control module 450, and processing logic 460.

[0032] Input/output module 410 is configured to allow for communication between privacy management module 140 and various users and other components

of virtual social network 110. Input/output module 410 may be configured to receive information via a communication network 150, such as the Internet or an intranet.

[0033] Authentication module 420 is configured to verify an individual's identity in virtual social network 110. Identifying an individual as a particular user of virtual social network 110 (e.g., user 160A) allows that individual to perform certain operations available to user 160A, such as accessing certain profiles, accessing certain communities, accessing certain content, etc. Authentication may occur, for example, through verification of a user name and password supplied by the individual. The user name and password may be compared to the user names and passwords stored in an authentication database, which may be independent of, or incorporated into, authentication module 420.

[0034] Friend set database 430 is configured to receive and store information concerning friend sets. Such information may include the name of the friend set, the members of the friend set, the set permissions associated with the friend set, and the like. The information concerning each user's personal friend set may be managed by the user using personal friend set module 220 illustrated in FIG. 2. Friend set database 430 is further configured to automatically receive updated information concerning revised friend sets. As discussed above, friend sets may be used by the user to manage groups of individuals. Access by a friend set may be determined by a set permission associated with the friend set, by user designation in association with content posted by the user, or the like.

[0035] Preferences database 440 receives and stores user preferences governing access to certain content provided by the user. The associations between the content and the user preferences allow the user to selectively control access. A user may post a blog entry, for example, which includes a plurality of photographs. The user can control who will be able to access each photograph by designating a different user preference for each one. For example, the user may limit access to certain photographs, so that only his immediate family and close friends can see them. The user may also allow a default preference to apply to the rest of the photographs posted in the user's blog entry. Each user preference is associated, as designated by the user, with specific content and stored in preferences database 440.

In various embodiments, the user may update a user preference associated with the content. Preference database 440 may automatically update to reflect the updated user preference associated with the designated content.

[0036] Access control module 450 manages and enforces user preferences concerning access to the content posted by a user. An individual wishing to access content posted by the user submits a request for access to that content. Submitting a request may include clicking on a link, clicking on a button, submitting a form request, subscribing to a content feed, etc. The request is received by access control module 450, which operates in conjunction with preferences database 440 to determine whether or not to grant access to the requesting individual. If the user preference for the content allows public access, the requesting individual is automatically granted access to the content. If the user preference is set to private (e.g., accessible only to the user), the requesting individual is automatically denied access. If the user preference restricts access to specific individuals or friend sets, access control module 450 determines whether the requesting individual is one of the individuals authorized to access the content.

[0037] In various embodiments of the present invention, the requesting individual must be authenticated by authentication module 420 as a user of virtual social network 110. The requesting individual may further be required to join a community. For example, the user may designate a user preference to allow access only to members of a community. Access control module 450, therefore, would only grant access to an individual if that individual has been authenticated as being a user of virtual social network 110 and a member of the required community. In various embodiments of the present invention, the user may limit access to a specific friend set. In that case, the requesting individual must be a member of the user's friend set, as stored in friend set database 430, in order for access control module 450 to permit access to the desired content.

[0038] The requesting individual may also contact the user through personal messages module 230 (FIG. 2) or other means to request access to certain content. The user may choose to grant the request by updating a user preference to authorize the requesting individual, updating a user preference to allow public access,

updating a friend set to include the requesting individual, or the like. Friend set database 430 and preferences database 440 may be automatically updated, and access control module 450 can act on the updated information to allow the requesting individual to access the content.

[0039] Access control module 450 may also enforce community rules. Determined and set by a community moderator or the like, community rules may allow content (including profiles) posted in the community to be accessed by the general public, by members of the virtual social network only, by members of communities in the virtual social network only, by members of a particular community only, etc. For example, a user profile (e.g., user profile 125A illustrated in FIG. 2) posted in a particular community (e.g., community A) may only be accessed by members of that particular community and may not be accessed by anyone outside the community. That user profile is exclusive to that particular community. Therefore, an individual browsing a community B may be able to view user profile 125B (FIG. 1) associated with community B, but may not be able to view user profile 125A.

[0040] Alternatively, community rules may allow for a user profile posted in the particular community to be accessible by members of related communities. For instance, the community rules of community B may allow for user profiles in community B to be accessed by members of community A. Such access by related communities may or may not be reciprocated by the related communities. Using the above example, access to user profiles of community A members may still be denied to members of community B who are not also members of community A. Profile access between two communities, therefore, may be reciprocal (two-way access), nonreciprocal (one-way access), or exclusive (no access).

[0041] Processing logic 460 is configured to execute a variety of operations required by the various components of privacy management module 140. In various embodiments, processing logic 460 may be implemented through use of microprocessors, memory, firmware, and/or software.

[0042] FIG. 5 is a flowchart illustrating a method for managing the privacy of user content in virtual social network 110 (FIG. 1), according to an exemplary

embodiment. In step 510, content is received from a user. The content may be uploaded by the user, posted by the user, or linked to through an activity module by the user in a community, for instance. In various embodiments, the content may be associated with an indication, such as a link, button, etc., visible to other individuals in virtual social network 110.

[0043] In step 520, the content provided by the user is associated with a user preference governing access to that content, and that user preference is stored. However provided, each separately identifiable content is associated with a user preference. In some embodiments of the present invention, virtual social network 110 may provide a default user preference or default set of user preferences to be used in the absence of a user designation to the contrary. Privacy management module 140 can allow users to customize such default user preferences. Specifying a default user preference allows the user to control access without having to designate the same commonly-used user preference repeatedly. In various embodiments, the user may be prompted to designate a user preference upon providing content. Alternatively, the user may designate user preferences without being prompted.

[0044] Further, information concerning the association between the content and the user preference is stored to preferences database 440 illustrated in FIG. 4. Preferences database 440 serves as a repository for information concerning the user preferences and their associations with particular content. Other components of virtual social network 110, such as access control module 450 (FIG. 4), may refer to preferences database 440 in making determinations involving content and associated user preferences. If the content is posted in a community, access to the content may be further constrained by the preferences, or rules, of the community. Associations with community rules may also be saved to preferences database 440 and may be used by access control module 450 in making determinations concerning access to the content.

[0045] In step 530, a request for access to content is received by access control module 450. In some embodiments, an individual in virtual social network 110 may have been alerted to the likely presence of the content by an indicator, such as a hyperlink, hyperlink address, or button. That individual may submit a request for

the content may include simply clicking on the indication, entering the hyperlink address, or the like. For example, an individual may click on a hyperlink for "Photos" to request access to photographs posted by the user.

**[0046]** In step 540, a determination is made as to whether the requesting individual is allowed access to the content based on user preferences. Using the information concerning user preferences associated with the content as saved in preferences database 440, access control module 450 determines whether the requesting individual is authorized by the user to access the content. In some embodiments of the present invention, this may require authenticating the identity of the requesting individual through authentication module 420. Various embodiments of the present invention may further require, for example, that the requesting individual be registered in virtual social network 110, be a member of at least one community, or have a personal profile. Since the user may choose to designate a friend set rather than a list of individuals, access control module 450 can operate in conjunction with friend set database 430 to determine whether the requesting individual is a member of the designated friend set.

**[0047]** If the determination is made in step 540 that the requesting individual is authorized to access the content, then in step 550, the content is provided. For example, a screen displaying the content may automatically appear, the link to the content may become operative, the content may be unblocked or otherwise made available to the requesting individual. In various embodiments of the present invention, the requesting individual must also satisfy the restrictions of virtual social network 100 and/or community rules before being allowed to access the content. Using the above example, an individual requesting access to a user's photographs may have been authorized by the user to view five of photographs posted by the user. In step 550, then, the requesting individual may be provided with five hyperlinks to the five photographs for which the individual is authorized to access. Alternatively, the individual may be provided with the five photographs.

**[0048]** If the determination is made in step 540 that the requesting individual is not authorized to access the content based on user preference, step 560 follows. In step 560, access to the content is denied. Access to the content remains blocked or

otherwise unavailable to the requesting individual. A message or a screen display indicating that access is denied may be provided to the requesting individual to indicate that the link to the content is inoperative, for instance. Alternatively, the requesting individual may not receive any indication of the content to which the individual is denied access. Referring to the above example, an individual may have been authorized to view five photographs, but there may be an additional two photographs that the individual is not authorized to access. The requesting individual, therefore, may only receive indication or be provided with the five photographs. In another example, if an individual has not been authorized to view any photographs, then that individual will not receive any indication that there are any photographs posted by the user. The "Photos" folder or page may appear empty, for instance.

[0049] In various embodiments of the present invention, a requesting individual who was denied access may submit another request for access to the content. Because a user may change user preferences (e.g., from restricted to public access) at any time, a request made after user preferences have updated may allow for the requesting individual to access the content. If the user decides to allow the requesting individual access to the content, the user can update the associated user preference (or friend sets). The updated user preference is associated with the content and, therefore, governs access to the content. If the user does not adjust the associated user preference or friend set, the content remains unavailable to the requesting individual.

[0050] It will be understood that the methods of the invention are not necessarily limited to the discrete steps or the order of the steps described with respect to FIG. 5. While the present invention has been described in the context of a series of exemplary embodiments, these descriptions are not intended to limit the scope of the invention to the particular forms set forth herein. To the contrary, the present descriptions are intended to cover such alternatives, modifications, and equivalents as may be included within the spirit and scope of the invention as defined by the appended claims and otherwise appreciated by one of ordinary skill in the art.

## CLAIMS

What is claimed is:

1. A method for managing the privacy of user content in a virtual social network, the method comprising:  
receiving content specified by a first user of the social network;  
associating a user preference with the content, the user preference limiting who is authorized to access the user content;  
receiving a request from a second user for access to the user content; and  
determining from the user preference whether the second user is authorized to access the user content.
2. The method of claim 1 wherein associating the user preference with the content includes associating a default user preference with the content.
3. The method of claim 1 or 2 wherein associating the user preference with the content includes receiving from the first user an indication of who is authorized to access the user content.
4. The method of claim 3 wherein the indication of who is authorized to access the user content includes an individual.
5. The method of claim 3 or 4 wherein the indication of who is authorized to access the user content includes the members of a friend set.
6. The method of claim 3, 4, or 5 wherein the indication of who is authorized to access the user content includes the members of a community.

7. The method of claim 1, 2, 3, 4, 5, or 6 further comprising authenticating the identity of the second user prior to determining whether the second user is authorized to access the user content.
8. The method of claim 1, 2, 3, 4, 5, 6 or 7 wherein the user preference further limits who is authorized to post a comment associated with the user content.
9. The method of claim 1, 2, 3, 4, 5, 6, 7, or 8 wherein the user preference further limits what type of content can be posted as a comment associated with the user content.
10. A system for managing the privacy of user content in a virtual social network, the system comprising:
  - an input module configured to receive content specified by a first user of the social network;
  - a database configured to store a user preference associated with the content, the user preference limiting who is authorized to access the user content; and
  - an access control module configured to determine from the user preference whether a second user is authorized to access the user content.
11. The system of claim 10 wherein the user preference comprises a default user preference.
12. The system of claim 11 wherein the default user preference was previously designated by the user.
13. The system of claim 10, 11, or 12 further comprising an authentication module configured to authenticate an identity of an individual in the virtual social network.

14. The system of claim 13 wherein the control module is further configured to determine that the individual is a member of at least one friend set associated with the user based on the authenticated identity of the individual.
15. The system of claim 13 or 14 wherein the control module is further configured to determine that the individual is a member of at least one community based on the authenticated identity of the individual.
16. The system of claim 10, 11, 12, 13, 14, or 15, further comprising a friend set database configured to store information concerning friend sets associated with the user.
17. A computer-readable storage medium having stored thereupon executable computing instructions for performing a method comprising:
  - receiving content specified by a first user of the social network;
  - associating a user preference with the content, the user preference limiting who is authorized to access the user content;
  - receiving a request from a second user for access to the user content; and
  - determining from the user preference whether the second user is authorized to access the user content.

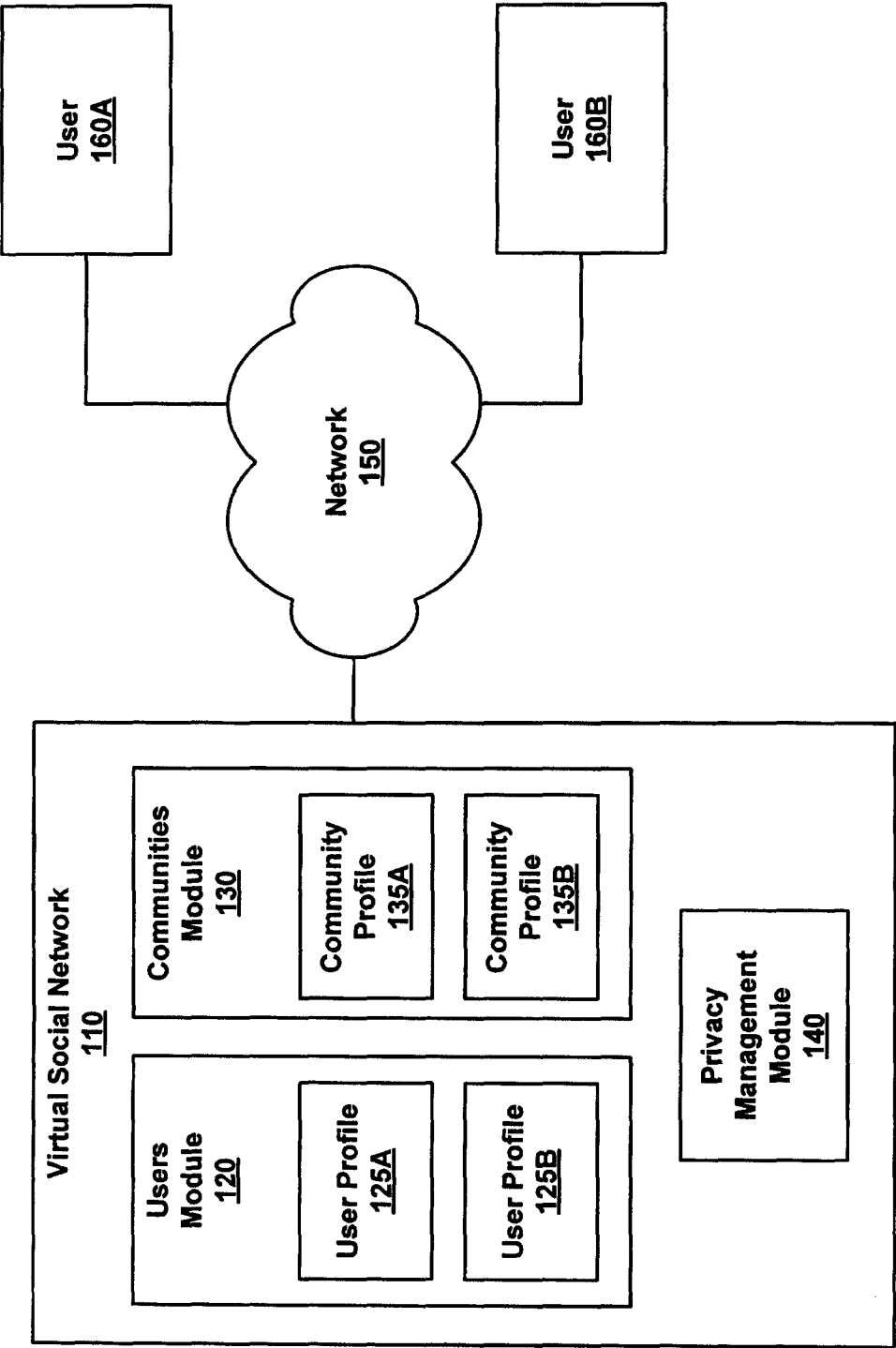


FIG. 1

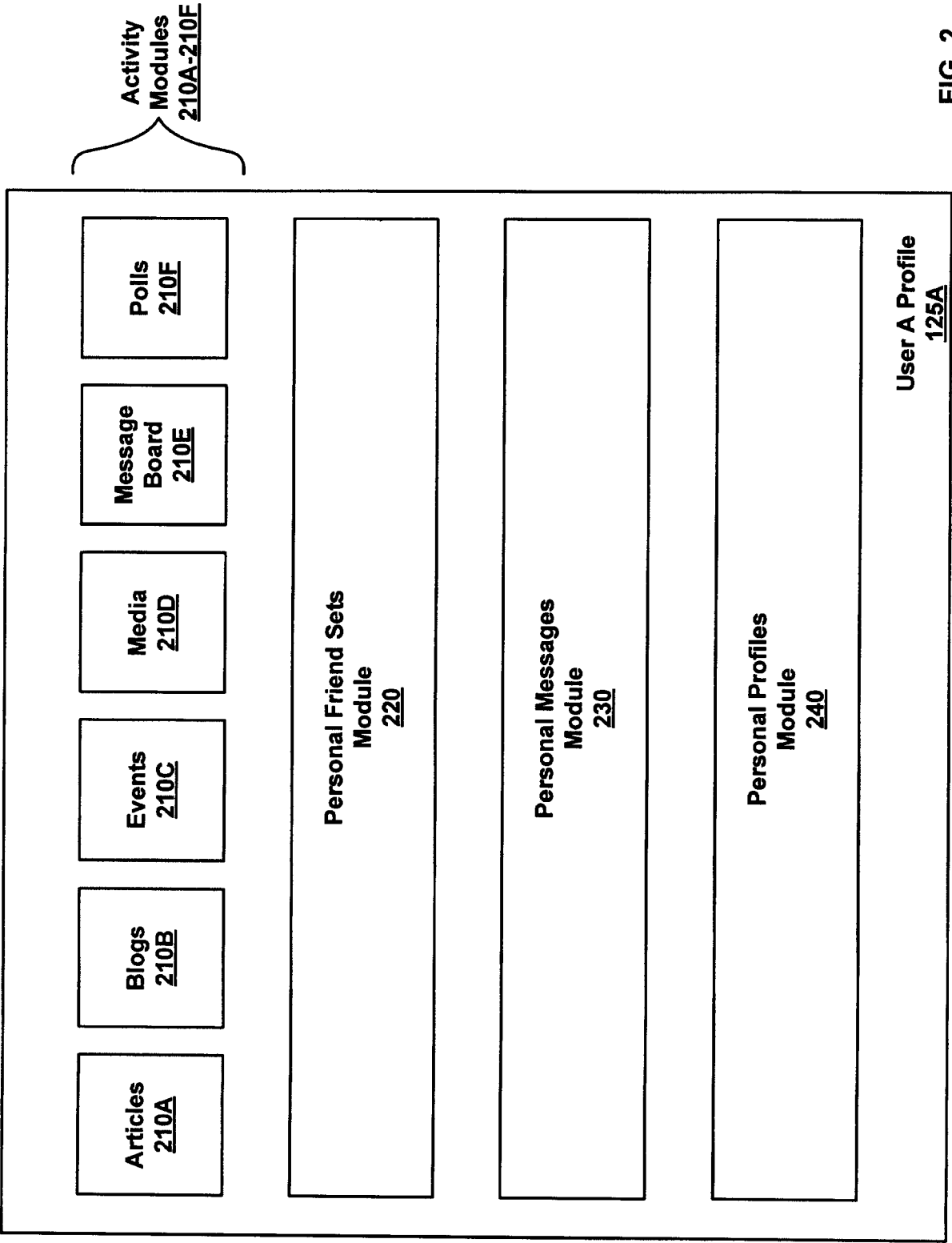


FIG. 2

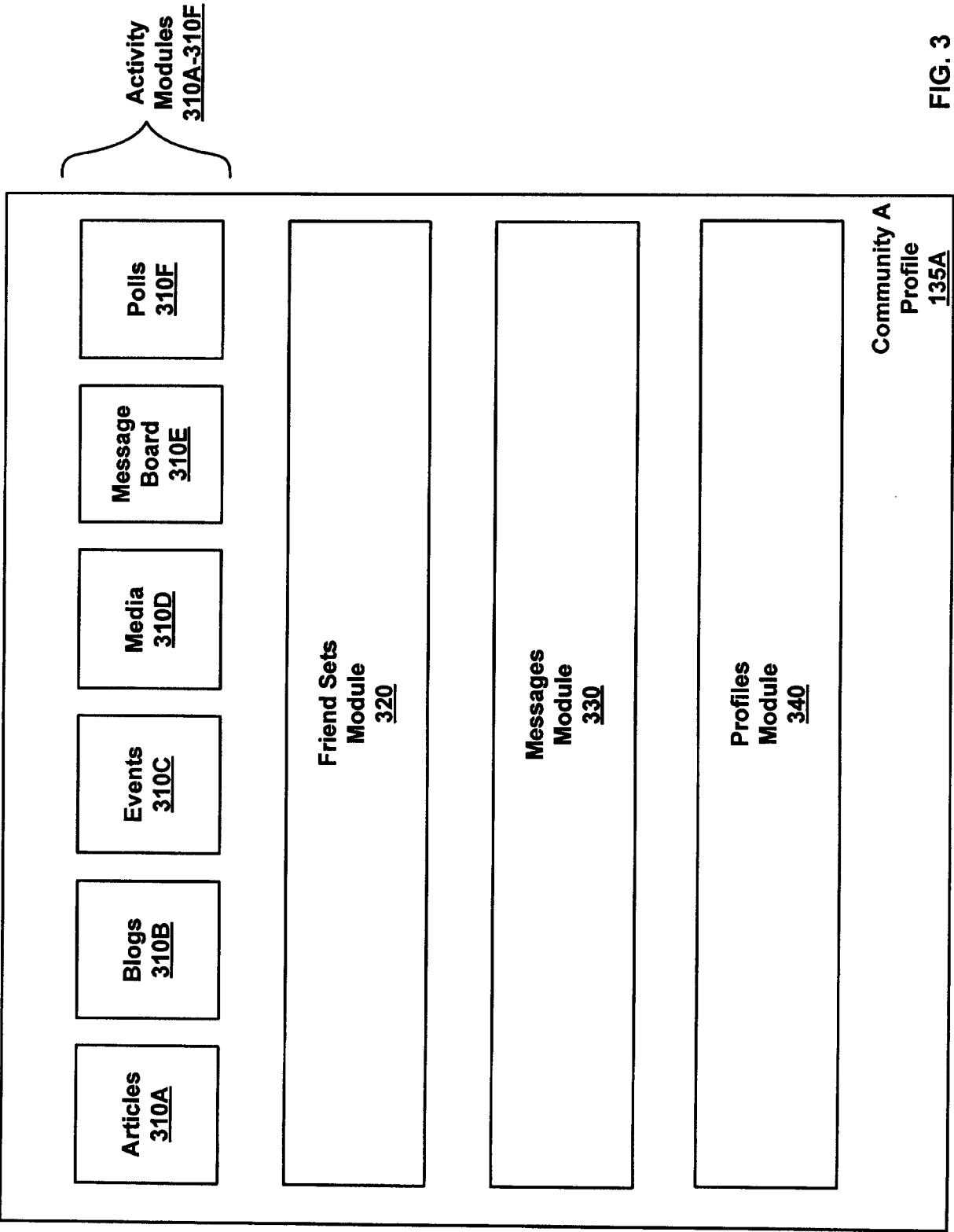


FIG. 3

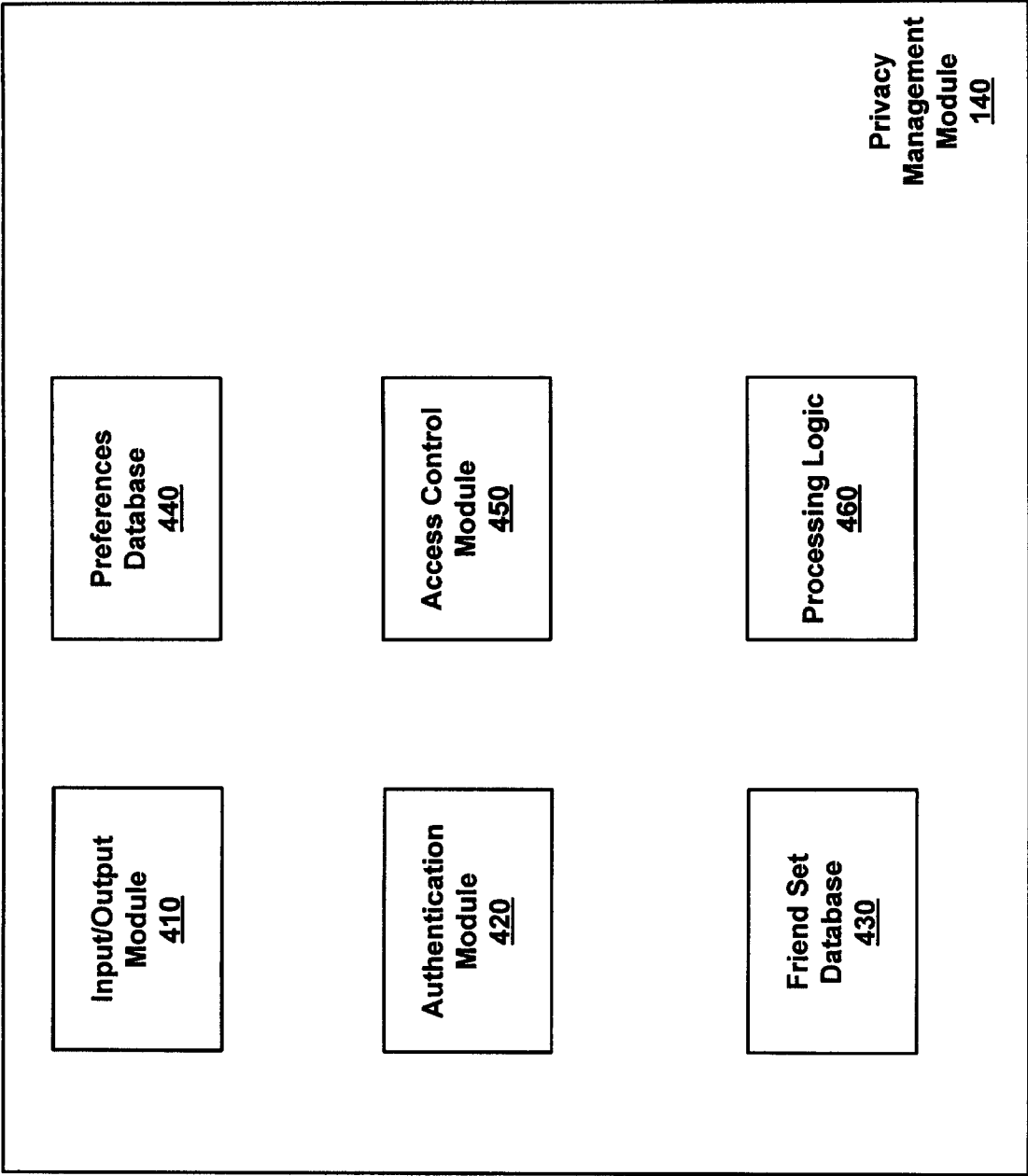
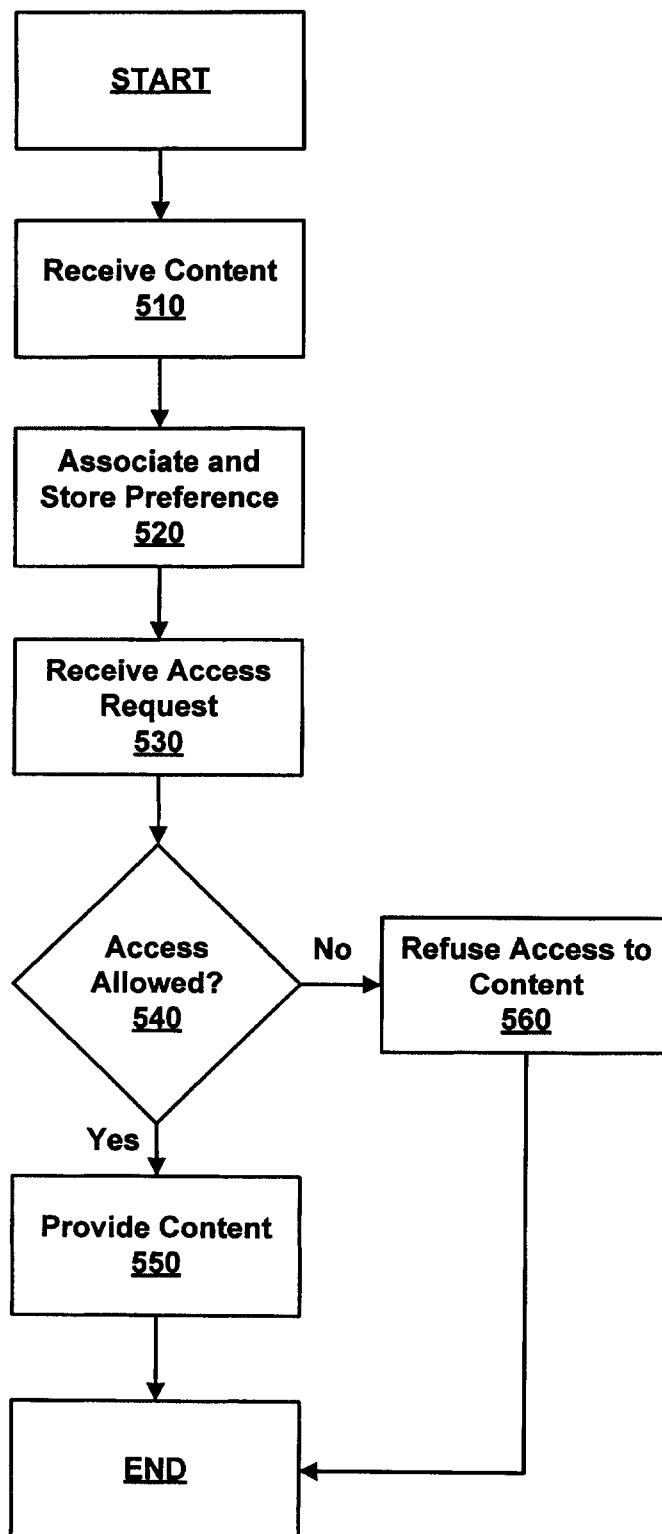


FIG. 4

**500****FIG. 5**

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/CA2007/001918

| <b>A. CLASSIFICATION OF SUBJECT MATTER</b><br><b>IPC: G06F 21/00 (2006.01)</b><br>According to International Patent Classification (IPC) or to both national classification and IPC   |  |                       |
|---|--|-----------------------|
| <b>B. FIELDS SEARCHED</b><br>Minimum documentation searched (classification system followed by classification symbols)<br>IPC: G06F , H04L<br>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched<br>Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)<br>Delphion, Pluspat, IEEEExplore, Google (social, network/networking, site, virtual, community, privacy, protect, content, information, access, control, authoriz*, authentica*, list, friends)        |  |                       |
| <b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>   |  |                       |
| Category*   | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
| X   | US 2005/0209999 A1 (Jou) 22 September 2005 (22-09-2005)<br>* whole document *  | 1-17                  |
| X   | US 2005/0198031 A1 (Pezaris et al.) 8 September 2005 (08-09-2005)<br>* whole document *  | 1-17                  |
| X   | US 2005/0267766 A1 (Galbreath et al.) 1 December 2005 (01-12-2005)<br>* whole document *   | 1-5, 7, 10-14, 16, 17 |
| X   | US 2006/0218225 A1 (Hee Voon et al.) 28 September 2006 (28-09-2006)<br>* abstract *<br>* paragraphs [0023]-[0025], [0030]-[0034], [0050]-[0054], [0065], [0081] *  | 1, 3, 4, 6, 10, 17    |
| <input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.   |  |                       |
| * Special categories of cited documents :<br>"A" document defining the general state of the art which is not considered to be of particular relevance<br>"B" earlier application or patent but published on or after the international filing date<br>"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)<br>"O" document referring to an oral disclosure, use, exhibition or other means<br>"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<br>"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<br>"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<br>"&" document member of the same patent family |                       |
| Date of the actual completion of the international search<br>9 January 2008 (09-01-2008)  | Date of mailing of the international search report<br>11 February 2008 (11-02-2008)  |                       |
| Name and mailing address of the ISA/CA<br>Canadian Intellectual Property Office<br>Place du Portage I, C114 - 1st Floor, Box PCT<br>50 Victoria Street<br>Gatineau, Quebec K1A 0C9<br>Facsimile No.: 001-819-953-2476   | Authorized officer<br>Jeffrey Orser 819- 934-2669  |                       |

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/CA2007/001918

| C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT |  |                       |
|---|--|-----------------------|
| Category*   | Citation of document, with indication, where appropriate, of the relevant passages   | Relevant to claim No. |
| A   | <p>US 2006/0184997 A1 (La Rotonda et al.) 17 August 2006 (17-08-2006)</p> <p>* abstract *</p> <p>* paragraphs [0002]-[0006], [0018]-[0020], [0044] *</p> <p>* claim 1 *</p> <p>---</p> | 1, 10, 17             |
| A   | <p>US 2006/0021009 A1 (Lunt) 26 January 2006 (26-01-2006)</p> <p>* whole document *</p> <p>---</p>   | 1, 10, 17             |

**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.  
**PCT/CA2007/001918**

| Patent Document<br>Cited in Search Report | Publication<br>Date | Patent Family<br>Member(s)  | Publication<br>Date  |
|---|---------------------|---|--|
| US2005209999                              | 22-09-2005          | US2005210409 A1<br>WO2005092014 A2  | 22-09-2005<br>06-10-2005   |
| US2005198031                              | 08-09-2005          | US2005197922 A1<br>US2005198305 A1  | 08-09-2005<br>08-09-2005   |
| US2005267766                              | 01-12-2005          | NONE  |  |
| US2006218225                              | 28-09-2006          | US2006218153 A1   | 28-09-2006   |
| US2006184997                              | 17-08-2006          | US7269590 B2<br>US2005171799 A1<br>US2005171832 A1<br>US2005171954 A1<br>US2005171955 A1<br>US2006184578 A1<br>US2006230061 A1<br>WO2005074441 A2<br>WO2005074443 A2<br>WO2005074444 A2<br>WO2005074445 A2<br>WO2005076184 A1 | 11-09-2007<br>04-08-2005<br>04-08-2005<br>04-08-2005<br>04-08-2005<br>17-08-2006<br>12-10-2006<br>18-08-2005<br>18-08-2005<br>18-08-2005<br>18-08-2005<br>18-08-2005 |
| US2006021009                              | 26-01-2006          | CN101036366 A<br>EP1782604 A1<br>WO2006019752 A1  | 12-09-2007<br>09-05-2007<br>23-02-2006   |