**A conceptual analysis of group privacy in the virtual environment**

by

Nanda Surendra

Assistant Professor of MIS

College of Business & Economics

West Virginia University

Morgantown, WV 26506-6025

nanda.surendra@mail.wvu.edu

and

A. Graham Peace

Associate Professor of MIS

College of Business & Economics

West Virginia University

Morgantown, WV 26506-6025

graham.peace@mail.wvu.edu

Submitted for review to the ***International Journal of Networking and Virtual Organisations (IJNVO)* on** November 1, 2007

Special Edition on: "Privacy in a Virtual Environment: Theory & Practice."

*Guest Editor*: Regina Connolly, Dublin City University, Ireland

**Author Biographies**

**Dr. Nanda Surendra**

Dr. Surendra is an Assistant Professor of MIS at the College of Business & Economics, West Virginia University. His current research is in the area of systems design and development, focusing on agile systems development methodologies. He has a paper forthcoming in *Information Technology and Management*. He teaches Business Applications Programming, Systems Analysis, Systems Design & Development courses.

**Dr. A. Graham Peace**

Dr. Peace is an Associate Professor of MIS at the College of Business & Economics, West Virginia University. His research interests focus on the area of Information Ethics, and he has published papers in several journals, including *Communications of the ACM*, the *Journal of Management Information Systems*, and the *Journal of Computer Information Systems*. He also co-edited the book *Information Ethics: Privacy and Intellectual Property*. Dr. Peace primarily teaches courses on database management systems, systems analysis, and information ethics.

**A conceptual analysis of group privacy in the virtual environment**

**Abstract**

While individual privacy has been the subject of considerable research in both the face-to-face and virtual environments, the idea of “group privacy” has received less attention. Proponents advocate the idea of group privacy on the following two principles:

* Group privacy should protect the need of people to come together to exchange information and share feelings. In this process, people reveal themselves to each other and rely on the others in the group to keep this information within the group.
* Combination of information disseminated about a group and the realization that a certain individual is a member of that group can potentially violate that individual’s privacy.

In the virtual environment, group privacy may be as important as individual privacy, given the popularity and pervasiveness of discussion forums, e-mail listservs and “social networking” websites, such Facebook and MySpace. This paper provides an overview of group privacy, the impact of virtual communities on group privacy, and a discussion of potential future research in this important area.

**1. Introduction**

Humans have always been social beings, so it is not surprising that many people use new technologies to form or enhance communities. The Internet is no exception, with billions of emails sent each day, and social networking sites, such as Facebook and MySpace, becoming household names. One of the great benefits of technology is that it eliminates the boundaries imposed by distance and time, thus allowing people to form groups (virtual communities) in which they can share opinions and knowledge with those who have similar interests. However, the same technology that facilitates this “group-making” can also create threats to the group members’ privacy, on both a personal and group level. As stated by Richard Mason, in his seminal paper on the ethical issues of the information age, technology’s capacity to capture and store information, combined with the increased value of that information in decision-making by companies, governments, etc., has created a major threat to privacy, especially in the age of the Internet (Mason, 1986).

While individual privacy has been the subject of considerable research in both the face-to-face and virtual environments, the concept of “group privacy” has received little to no attention. A search using the keywords “Privacy” and “Information Technology” in one of the premier research databases, ABI Inform, located 340 scholarly journal articles. In contrast, a search using the keywords “Group privacy” and “Information Technology” located 0 articles. There was only one scholarly article that used the term “group privacy” (Barton, et al, 2005). However, the authors of this article used the term “group privacy” only once, and the concept was not a main focus of the paper.

Proponents advocate the idea of group privacy on the following two principles:

* Group privacy should protect the need of people to come together to exchange information and share feelings. In this process, people reveal themselves to each other and rely on the others in the group to keep this information within the group (Bloustein, 1978).
* The combination of information disseminated about a group, and the realization that a certain individual is a member of that group, can potentially violate that individual’s privacy (Gavison, 1980).

In the virtual environment, group privacy may be as important as individual privacy, given the pervasiveness of discussion forums, e-mail listservs and “social networking” websites. A recent high profile case involving the daughter of a candidate for the United States presidency serves as an example of a group privacy violation, and highlights the heightened vulnerability of social networking sites to such violations (New York Times, 2007). The daughter of the candidate stated a few of her political preferences on her Facebook page that she made accessible only to group-members belonging to her high school and the college she planned to attend. A member of the college group took a “snap shot” of her page and made the page’s contents available to everyone who had access to the internet. This action violated the candidate’s daughter’s “group privacy” expectation that she had shared her political views only with two groups (her fellow school and college members), and not with society as a whole.

This paper conceptually addresses the following issues:

1. How group privacy is defined,
2. The benefits and limitations of group privacy,
3. A comparison of face-to-face and virtual groups, with respect to group privacy,
4. Threats to group privacy in the virtual environment,
5. Measures to safeguard, and prevent violations of, group privacy in the virtual environment,
6. The current practices and policies of prominent social networking sites regarding group privacy,
7. Potential areas of future research in the area of group privacy and virtual communities.

**2. Group privacy: A definition**

Privacy is a difficult thing to define, as it means different things to different people. The concept of a “right to privacy” can also be difficult to establish. Walters (2001) states that longstanding moral and legal debates about privacy and the right to privacy are not surprising, since a community’s agreed-upon conception of norms are a social construction. We generally do not recognize privacy’s importance, until taken away. It is also a personal right taken for granted until someone infringes on it. In a similar manner, it is difficult to develop a single, common definition of “group privacy,” since the definition of group privacy, and the right to group privacy, is dependent upon socially constructed norms within a group.

Philosophers have generally defined privacy along the following lines:

1. A claim, entitlement, or right of the person to determine what personal information about one self may be communicated to others.
2. Control over access to information about oneself.

These definitions focus on the individual. William Prosser (1960) argued that privacy is not an independent value per se, but a complex of four torts:

* intrusion upon one’s solitude or private affairs,
* public disclosure of embarrassing private facts,
* publicity which places one in a false light in the public eye, and
* appropriation of one’s name or likeness for personal advantage.

Again, the focus is on the individual. Brandeis and Warren introduced the first legal structure of the concept of privacy (Prosser, 1960). However, they primarily dealt with the individual right to privacy (the “right to be let alone”). Bloustein (1979) was the first to introduce the idea of group privacy (the “right to huddle”). He stated that group privacy is a form of privacy that people seek in their associations with others. Group privacy is an attribute of individuals in association with one another within a group, rather than an attribute of the group itself. Bloustein (1979) describes group privacy as follows (page 125):

“The interest protected by group privacy is the desire and need of people to come together, to exchange information, share feelings, make plans and act in concert to attain their objectives. This requires that people reveal themselves to one another – breach their individual privacy – and rely on those with whom they associate to keep within the group what was revealed. Thus, group privacy protects people’s outer space rather than their inner space, their gregarious nature rather than their desire for complete seclusion. People fashion individual privacy by regulating whether, and how much of, the self will be shared; group privacy is fashioned by regulating the sharing or association process.”

Bloustein (1979) addressed the issue of regulating or protecting group privacy with a set of questions (page 126):

* Who are the parties to, and what are the purposes of, the association?
* What is the subject of the confidence?
* How long is it intended that the confidence be maintained?
* Who are the parties seeking access to the group confidence and for what purpose?

Group privacy is not independent of individual privacy, but is related to the individual privacy of members who constitute the group. A combination of information disseminated about a group and the realization that a certain individual is a member of that group can potentially violate that individual’s privacy. The size of a group plays a role in whether information about the group can be traced to an individual member. For example, negative perceptions about a university (such as being ranked by a national magazine as a “party school”) are not particularly “traceable” to an individual student of that university. On the other hand, if a college fraternity with 15 members has the same negative designation, then each person identified as a member of that fraternity is likely to be more strongly “branded” with the same negative designation.

A second factor that determines whether information about a group could potentially violate an individual’s privacy is the specificity of the information. For example, if the information specifies age, gender, and ethnicity of the people within a group to whom it pertains, then the “traceability” of the specific individual, and the resultant violation of that individual’s privacy, increases. A third factor in the relationship between group privacy and individual privacy is a member’s strength of affiliation with a group. For example, a student’s affiliation with a fraternity or sorority is usually much stronger than his or her affiliation with a student recreational group.

**3. Ethics and group privacy**

Philosophical ethics can be used to analyze the pros and cons of privacy, both in an individual and group context (Ermann and Shauf, 2003). Different normative frameworks of ethics can help guide the discussion about what ought to be done, regarding privacy. Two well-known ethical frameworks are the utilitarian and deontological models. Each can be used to study the role of privacy in the group environment.

The utilitarian model states that, of all the actions available to us, we are obliged to choose the action that maximizes the greatest good for the greatest number (Hospers, 2003). The focus is on the consequence of the action, i.e. the positive and negative effects of that action. The utilitarian model’s recommendation on group privacy will be situational. If the greatest good is achieved by more access to information, then the recommendation will be to reduce group privacy. Conversely, if the greatest benefit can be created through the group remaining private, then that will be the ethical act. With the utilitarian model, we need to consider long-term implications in addition to just the short-term effects. Also, while maximizing social utility, we need to minimize negative side effects.

For example, in the case of a group of young adults involved in a social networking site that discusses music, it may be that a reduction of privacy could be seen as a benefit to all involved. Corporations selling music will be able to gain valuable marketing research, thus improving sales. The individuals involved will have better options for purchase (as those options will be tailored to their interests), thus improving their enjoyment. There is little harm created, so the lack of group privacy can be seen as ethical. However, a group of individuals using a social networking site to discuss political change in a repressive regime may face serious consequences, if their group privacy is violated. In this case, it might be argued that reducing the group’s privacy is unethical. The challenge is balancing the benefits of protecting privacy with the costs of privacy. The benefits of privacy are that it ensures people’s participation in society, politics, and commerce without fear that the information they provide will be used in ways that are detrimental to them. A potentially serious negative consequence of privacy is that socially undesirable actions may take place outside of the knowledge of the proper authorities (e.g. planning a terrorist attack, or sharing of child pornography).

The deontological framework is focused on the act itself (Rachels, 2003). Is the *act* ethical or unethical? Consequences are unimportant. The ethical nature of the act can be determined through a logical analysis and consideration of the rights and duties involved. Some acts are simply unethical by their nature, such as lying, stealing, killing, etc. The Kantian model of deontology states that people should always be treated as ends, not as means to accomplishing an objective. Kant believed that autonomy was a quintessential human right and that a human being should never be treated “merely as a means.” The Kantian model’s recommendation on group privacy will likely be absolute – that it should not be violated under any circumstance. Such a violation will result in treating the person or group whose group privacy has been violated as a means to achieve some other objective.

**4. Benefits of group privacy**

Group privacy can provide many benefits. Some of the reasons for enabling and fostering group privacy are the following:

* To create an environment that is conducive to innovative thinking and the development of ideas. If members of a group suspect that their ideas might be “leaked” by other group members, then they are unlikely to share innovative ideas with the group (Keenan, 2005).
* To encourage group members to be candid and honest with one another. It is usually assumed that group members should always cooperate and support one another to be productive as a group. However, for a group to be productive, it is vital that members also be able to question one another without inhibition – to not get boxed into “groupthink” (Schiano and Weiss, 2006).
* To prevent persecution and/or discrimination, based on group membership.
* Lack of group privacy could lead to a loss of autonomy (inability to put on a “different face” in different groups) (Keenan, 2005).
* To ensure that the right person or people get credit for their contribution. If the information shared with members of a group are broadcast widely outside the group, then the member or members who made the contribution may not receive credit for that contribution.
* While the right to be “let alone” protects the integrity and dignity of the individual; the right to group privacy in one’s association assures the success and integrity of the group purpose (Bloustein, 1979).

**5. Limitations of group privacy**

Group privacy does have its limitations. Equation of privacy with private ownership leads to the potential decay of group commonality and its public amenities. A group benefits when members of the group agree to collective ownership of resources and ideas. If the welfare of individuals is conceived as the ultimate end for all members of a group, then the group might be less effective in carrying out its collective mission and objectives.

Also, all individuals do not necessarily want privacy. As indicated by the success of various credit card “loyalty” programs, millions of consumers want to have their purchases tracked so that they will be rewarded with benefits, such as free plane tickets or prizes (Garfinkel, 2000). The same might apply to group privacy. In some cases, group members might not want group privacy. There might be a benefit for members by announcing membership in a group (example, prestige from being accorded membership in an exclusive group). Conversely, there might be a benefit for the group by announcing that an individual with influence or prestige has joined the group as a member.

Group privacy may have the potential to infringe on freedom of information, i.e. preventing access to information to individuals and groups outside of that group who could be affected or benefit from that information. For example, when groups within governmental organizations prevent access to information based on group privacy considerations, the right and necessity of a democratic society to understand how their government works is affected. Group privacy may infringe upon the rights of those outside of the group to know what is taking place and/or being discussed. Similarly, preventing members of a group from stating what was discussed in the group (in the name of group privacy) might violate free speech rights of members.

Does group privacy serve as a fence to keep information within a group, or as a barrier that prevents productive interaction across groups? Group privacy could result in the boundaries of a group (and who could be granted membership) being so tightly defined that it prevents collaboration with other groups and inclusion of members who can provide perspectives that are different from the group’s dominant perspective. Such an overly tight definition might lead to “convergence” of a single perspective, resulting in possible stagnation. Granovetter (1982) argued the importance of weak ties, stating that they are essential for innovative behavior. Weak ties in the form of other groups and individuals that have few to no commonalities with a group serve as bridge to infuse new ideas and insights into the group. Schiano and Weiss (2006) identify group insulation and homogeneity of members’ social background and ideology as two main antecedents of groupthink and its attendant pitfalls.

A study on the how users configured privacy permissions in an interactive group support tool showed that privacy has to be balanced against increased transparency, to build trust among members within a group, as well as people external to the group who are important contributors to the group’s objectives (Patil and Lai, 2005). So, an overemphasis on group privacy could potentially undermine trust, leading to reduced effectiveness in accomplishing a group’s objectives.

Finally, group privacy needs to be balanced against the protection of social and national interests. Hence, there might be a need to violate group privacy to prevent anti-social or other undesirable groups from carrying out illegal acts, such as criminal or terrorist behaviour. This argument has gained in prominence in the United States, since the terrorist acts of 9/11 (Hartzel and Deegan, 2005).

**6.** **Comparing group privacy between face-to-face and virtual groups**

Virtual communities remove three barriers to the formation of groups and the ability of individuals to become members of a group (Sproull and Kiesler, 1986):

* 1. Geographical separation or distance: The physical separation of prospective members is no longer a constraint.
  2. Time: Since asynchronous communication is possible in the virtual environment, members can participate on their own time schedules.
  3. Social inhibitions: Social context cues (physical features, mannerisms, and cues regarding position and power) are reduced, in the virtual environment. This enables individuals having these inhibitions to participate more fully in virtual groups, as opposed to face-to-face groups.

There is also a difference in how the history of the group is stored. In a face-to-face group, records may or may not be kept. However, in most virtual groups, almost every comment is stored digitally, and often made easily accessible. The nature of the information age is that all chat room conversations, bulletin board postings, etc. are stored in digital form in a computer system. There’s little need for privacy protection, when a conversation is taking place between three or four people at a remote campsite. When those same three or four people are conversing in a chatroom or via email, an electronic record is made of every comment.

In summary, virtual groups remove the barriers that can reduce participation in face-to-face groups, and they also create an environment in which the conversations of the group may be more easily stored, monitored and disseminated. This allows for much greater participation in a group, but can also increase the threat to group privacy, as discussed further in the following section.

**7. Threats to group privacy in the virtual environment**

In the past, the biggest enablers of privacy were the physical barriers to access of information (geographical distance, limited number of copies, etc.) and human limitations (limited and short memory capacity, limited ability to search and find specific information in a large volume of data, etc.). High speed networking and connectivity, combined with virtually no limits on the number of electronic copies of a database that can be made, remove the physical barriers to accessing information. A computer’s ability to store vast amounts of data for extremely long periods of time, combined with programs that can quickly search and find requested information, remove the barriers to privacy imposed by human limitations.

Technology is not neutral. By its very nature, technology is intrusive. While technology can be used to advance privacy, it usually reduces privacy. It is becoming more difficult and more expensive to design and build systems that protect privacy (Garfinkel, 2000). Also, with advances in data storage technologies, centralized data accumulation of massive databases becomes easier. Concurrently, the ability to search massive databases and “make connections” (correct connections that actually exist, or incorrect connections through faulty data or logic) between disparate data items has increased, with advances in data warehousing and data mining technologies. These technological advances in the storage and access of massive quantities of data have reduced the cost and increased the reward for intrusion, and have also shifted the control over these data to fewer people (Rosenberg, 1969; Lessig, 2006).

Social inhibitors in face-to-face environments usually prevent members of a group from being disruptive or abusive to an extent that prevents the group from accomplishing its objectives. However, virtual groups offer the shield of anonymity that might be misused by some members, in an effort to cause disruptive actions. Also, in a virtual environment, much greater disruption can be caused by a much smaller number of disgruntled members.

In the virtual world, it is very easy to gain membership to multiple groups. Hence, it is very common for group membership overlaps - where two or more members belong to common groups. This leads to potentially inadvertent group privacy violations - when discussions and information that pertain to one group are inadvertently brought into another group, due to the common membership. Members may forget which group they are currently participating in, especially when conversations take place in a virtual environment, where there are no physical queues to remind the participants who has access to the conversation taking place.

Similarly, another threat to group privacy is the “degrees of connection” through overlapping group memberships. A member of a group may make his information available to another member of his group. However, if this second member belongs to another group and reveals his information, including his connections to a member of the second group, then some of the first member’s information could be revealed to a “second degree” connection (information that the first member may not want to reveal to anyone other than immediate or “first degree” connections).

When new members are inducted into face-to-face groups, the credentials of applicants can be physically verified (to determine if the person is who he claims to be) and existing members can determine if the applicant will be a good “social fit.” In the virtual environment, it is much easier for a masquerader, pretending to be someone that he or she is not, to gain membership and intrude into the group. Such intruders are a threat to the group’s privacy.

The relative richness of the media used by a virtual group could also determine the extent of the threat to group privacy. Typically, the richer the media, the greater the threat to privacy. The richest medium would be a social networking group using video, audio and images. A group using a discussion forum would be lower on the richness scale, since most topics and responses are textual. A group using a text-based e-mail listserv would be the leanest medium, since it mainly consists of textual messages and, unlike the discussion forum, does not allow “thread-based” discussion.

Finally, most virtual communities have tools whose objective is to enhance cooperation among members of the group. The implicit assumption behind the design of such tools is that cooperation is always good for the group. As Kling (1991) noted, disagreement among members is as much an everyday group phenomenon as agreement, and it has the potential to be equally constructive (e.g. by preventing “groupthink”). One common example of a cooperative tool used by virtual groups is a member calendar that is made accessible to all other members of the group. This calendar forces each member to make known the activities he or she has scheduled, as well as his or her “free time” – leading to the erosion of the individual’s privacy.

**8. Measures to safeguard, and prevent violations of group privacy in the virtual environment**

There are several measures that can be taken to ensure group privacy in the virtual world. First of all, verification of a person’s identity can be undertaken. Most companies (including credit card companies) have made the dangerous assumption that if a person provides the name, address, telephone number, some sort of government-issued identifier (such as social security number, in the United States), and mother’s maiden name of the person they claim to be, then he or she is that person. However, this is relatively easy information to obtain, as evidenced by the many cases of identity theft reported regularly in the news media. Biometrics may provide a more secure verification system, in time, but currently few sites use this technology for verification.

Misuse of data and infringement of a person’s privacy can start when data provided by a person are used for reasons other than what they were originally intended. One approach to safeguarding privacy is to vigorously implement the third principle of the U.S. Department of Health Education and Welfare’s Code of Fair Information Practices: preventing information about a person that was obtained for one purpose from being used or made available for other purposes, without the person’s consent (Smith, 1993). The question regarding access to information needs to be context sensitive. It should not be the question “Who are you?”, regarding the entity trying to collect and use information, but “What are you going to use it for?” Making this question a “real-time” question brings into consideration the possibility of obtaining real-time permission to use data.

Another measure to safeguard group privacy is to adopt a layered approach, by categorizing each member’s levels of privacy. Individual members will be given the option of allocating information about themselves into several categories, starting from least sensitive and going up to most sensitive, on the individual member’s own “sensitivity scale.” This allows access to the member’s information, based on the “level of privacy” that the individual has assigned to particular pieces of information. This layered approach to privacy is used by Facebook. The next step is to enable a member to provide his or her informed consent to releasing information he or she has designated at a higher level of privacy. When such information is requested, the individual can determine who wants the information and for what purpose, before making his or her decision to release or withhold information.

**10. The practice or non-practice of “group privacy” among prominent social networking sites**

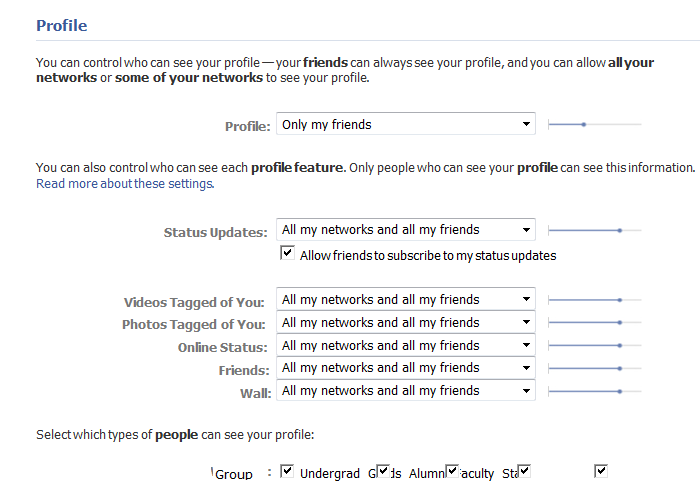
The Internet has spawned several prominent group networking sites. MySpace is the largest social networking site, with an estimated 75 million to 100 million registered users, at the beginning of the year 2007 (the difference in estimates is due to the existence of several million “fake accounts”). MySpace deals with privacy on an individual basis and does not provide options for enabling group privacy. A MySpace user’s potential privacy settings are as follows

**Profile Viewable By:** Only the people you select will be able to view your full profile and photos. Everyone else will only see your name, photo, location, and contact table.

The options for selecting who can view a user’s profile are “Everyone,” “Everyone 18 and over,” and “My friends only.”

Facebook (estimated 22 million registered users, as of August, 2007) has a privacy policy that is much more “group oriented,” stricter, and more granular (i.e. the user can use settings that allow or prevent access to specific Facebook individuals or groups), reflecting its origins as a online forum used within universities to enable students to find and meet other students with similar interests.

Until a year ago, Facebook only allowed a user to sign up if he or she was able to prove an affiliation with a university (in the United States, this was by verifying that a user had a .edu e-mail address). The privacy settings on Facebook are defined as follows (“network” is Facebook’s synonym for group):



Friendster, considered among the pioneering social networking sites catering to social connections and making friends, has the following statement regarding privacy:

To make your profile private, please go to your account settings. You can select who you want to make your full profile open to. You can make your profile accessible to friends, friends and 2nd degree friends or anyone. If someone tries to access your page outside of the selection you chose, they will see your limited (public) profile which contains your name, location, and primary picture.

Friendster introduces the concept of degrees of connection. A member directly selects another member to be designated as a first degree friend. Second degree friends are “friends of a members friends.” Third degree friends are removed by one more degree of connection. While Friendster improves on MySpace’s privacy policy by making members aware of enabling or disabling privacy settings to allow or prevent access to friends at different levels of connectivity, it does not provide options for privacy settings with regard to groups.

**10. Discussion**

Individual privacy has always been a concern. However, the concept of “group privacy” is relatively new. When taken in the context of virtual communities, made possible by the pervasiveness of information technology, group privacy becomes a more significant concern. Communications between group members are recorded and archived, and the increased value of information makes privacy violations more likely. The differences in the privacy policies of the various popular networking websites indicate that there is a lack of agreement as to how handle group privacy. While Facebook provides a very “group friendly” policy, MySpace is much more focused on the individual. Other networking sites have policies somewhere between the two.

The application of the major ethical theories to this situation does not necessarily help. Perhaps the easiest to apply is deontology, which can be used to make a case that group privacy should be protected as a fundamental right, no matter what the consequences. Therefore, from a deontological view, Facebook has an ethical policy, where an attempt is made to verify members, at least on some level, and group information is kept within the group, at the will of the individual member.

From a utilitarian perspective, the situation is much more context sensitive. Group privacy should be protected where this leads to a greater good, and should not be protected in situations where a lack of privacy would lead to greater benefits. It is difficult to use this theory to develop an overriding argument, but one could argue that the privacy level should be determined not by the members of the group, but by some regulatory entity that can include all stakeholders in the utilitarian calculation.

As more and more people join networking sites, and virtual groups become more a part of everyday life and less of a novelty, it is important that those providing the technology, and those regulating it, consider issues such as group privacy, since it could have legal and financial implications (Rosen, 2000). As members of virtual groups become more aware of the concept and implications of group privacy, companies that provide more options to enable group privacy may derive a competitive advantage and higher membership, compared to companies that pay less attention to group privacy.

From a practical perspective, members of virtual groups may consider a few of the following practices, to better protect group privacy:

* Use different identifiers or pseudonyms within different groups. This prevents a member from being identified within groups that have overlapping memberships.
* Set privacy levels at appropriate levels of granularity, regarding both who accesses information (are they authenticated?) and what is accessed by that person (do they have sufficient authorization?).
* Consider the group privacy trade-offs between the one-stop convenience of social networking sites (such as Facebook and MySpace) that allow textual communication along with photo, audio and video sharing, versus specialized service sites (such as Shutterfly, that allows sharing photos with specified groups and members). One-stop social networking sites are convenient but a greater threat to group privacy.

**11. Limitations and future research directions**

It is important that more research is done in this area, given the increasing pervasiveness of virtual communities. For a start, the definition and ethics of group privacy, and the impact of technology, requires a much more thorough analysis. Consensus needs to be reached on both a definition and an ethical standard for the concept of group privacy. Then, regulatory and technical standards need to be created to protect the privacy of the group, as well as the privacy of individuals. Once standards have been defined, it will be possible to study the major social networking sites, to determine where potential problems exist.

A primary limitation of this paper is that it is a conceptual analysis and not an empirical study. So, one obvious direction for future research is to collect data from virtual groups to study and strengthen the concept of group privacy, and its role in virtual communities. We have tried to explain the relation and difference between group privacy and the much better studied and understood individual privacy. Future research could shed more light on the connections and differences between these two – especially, with empirical studies.

Research issues we have raised in this paper that could be pursued further include the factors that impact group privacy (e.g. group size, group composition, richness of the medium used by a virtual group, etc.). How does group size impact group privacy? What type of medium (categorized from lean to rich) constitutes a greater threat to group privacy? What is the impact of type of membership (divergent versus convergent interests and backgrounds) on group privacy? These are all interesting questions that require further investigation.

Trust is also an important enabler of participation in a virtual community. Web merchants’ privacy policies regarding consumer data are considered key to establishing trust for online commerce (Gauzente, 2004; McRobb and Rogerson, 2004). In contrast, high levels of group privacy in virtual groups might be detrimental in building trust between group members, since it reduces transparency and the ability to get to know members of the group (Patil and Lai, 2005). An interesting concept for future research is studying how to establish a balance between group privacy and transparency in achieving trust, in virtual groups.

Maryam and Iverson (2006), using grounded theory, developed a concept map showing the centrality of individual privacy concerns in information sharing behavior. Future research could be undertaken using a similar concept map showing the centrality of group privacy. Figure 1 conceptualizes (a) how group size, composition, richness of the virtual group medium affect group privacy and (b) how group privacy affects trust among group members and group effectiveness at accomplishing its objectives.

Media Richness

Group Composition

Group Size

Group Privacy

Group effectiveness

Trust among group members

**Figure 1:** Concept map of group privacy

**12. Conclusion**

With more and more human interaction moving to the online world, it is critical that new ethical issues are evaluated and considered, prior to problems arising. With the rapid pace of change in the information technology discipline, both researchers and policy-makers need to ensure that people are protected from potentially unforeseen ethical problems, before new technologies become pervasive. The advent of the Internet has allowed humans to move their communities into a virtual world, changing the dynamics of privacy in the group setting. The social nature of humans practically guarantees that new technologies will be used to communicate and form communities. The concept of group privacy, and how group privacy should be dealt with in a virtual world, therefore requires further study, and should be a focal point for researchers and policy-makers, in years to come. **References**

Barton, B.,  [Byciuk](javascript:void(0);), S.,  [Harris](javascript:void(0);), C.,  [Schumack](javascript:void(0);), D.,  [Webster](javascript:void(0);), K. (2005) ‘The emerging cyber risks of biometrics’, *Risk Management*, Vol. 52, No. 10, pp. 26-30.

Bloustein, E. (1978) *Individual and group privacy*, New Jersey: Transaction Inc.

Ermann, M.D. and Shauf, M.S. (2003) ‘Philosophical ethics’, in Ermann, M.D. and Shauf, M.S. (eds.) *Computers, Ethics, and Society*, Oxford University Press, New York, NY, pp.2-3.

Garfinkel, S. (2000) *Database Nation*, New York: O’Reilly.

Gauzent, C. (2004) ‘Web merchants’ privacy and security statements: How reassuring are they for consumers? A two-sided approach’, *Journal of Electronic Commerce Research*, Vol. 5, No.3, pp.181-198.

Gavison, R. (1980) ‘Privacy and the limits of law’, *Yale Law Journal*, Vol. 89, No. 4, pp.21-71.

Granovetter, M.S. (1982) ‘The strength of weak ties: A network theory revisited’, in Marsden, P.V. and Lin, N. (eds.) *Social Structure and Network Analysis*, Sage, Beverly Hills, CA., pp.103-130.

Hartzel, K.S. and Deegan, P.E. (2005) ‘Balancing individual privacy rights and intelligence needs: Procedural-based vs. distributive-based justice perspectives on the Patriot act’, in Freeman, L. and Peace, A.G. (eds.) *Information ethics: Privacy and intellectual property*,Information Science Publishing, Hersey, PA, pp. 180-195.

Hospers, J. (2003) ‘The best action is the one with the best consequences’, in Ermann, M.D. and Shauf, M.S. (eds.) *Computers, Ethics, and Society*, Oxford University Press, New York, NY, pp. 3-11.

Keenan, K.K. (2005) *Invasion of privacy: A reference handbook*, Santa Barbara: ABC CLIO.

Kling, R. (1991) **‘**Cooperation, coordination and control in computer-supported work**’,** *Communications of the ACM*, Vol. 34, No. 12, pp. 83-88.

Lessig, L. (2006) *Code Version 2.0*, New York: Basic Books.

Mason, R (1986) ‘Four Ethical Issues of the Information Age’, *MIS Quarterly*, Vol. 10, No. 1, pp. 5-12.

McRobb, S. and Rogerson, S. (2004) ‘Are they really listening? An investigation into published online privacy policies at the beginning of the third millennium’, *Information Technology & People*, Vol 17, No. 4, pp. 442-461.

New York Times (2007) ‘Giuliani’s Daughter Shows Support for Obama, for a Time’ http://www.nytimes.com/2007/08/07/us/politics/07giuliani.html

Patil, S. and Lai, J. (2005) ‘Who gets to know what when: Configuring privacy permissions in an awareness application’, *Proceedings of the SIGCHI conference on Human factors in computing systems*, ACM, New York, NY, pp. 101-110

Prosser, W. (1960) ‘Privacy’, *California Law Review*, Vol. 48, No. 3, pp. 383-423

Razavi, M.N. and Iverson, L. (2006) ‘A grounded theory of information sharing behavior in personal learning space’, *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work*, ACM: New York, NY, pp. 459-468.

Rosen, J. (2000) *The unwanted gaze: The destruction of privacy in America*, New York: Random House.

Rosenberg, J. (1969) *The Death of Privacy*, New York: Random House.

Schiano, W and Weiss, J.W. (2006) ‘Y2K all over again: How groupthink permeates IS

and compromises security’, *Business Horizons*, Vol. 49, pp. 115—125

Smith, Robert (1993) ‘The law of privacy in a nutshell’, *Privacy Journal*, Vol. 19, No. 6, pp.50-51.

Sproull, L. and Kiesler, S. (1986) ‘Reducing social context cues: Electronic mail in organizational communication’, *Management Science*, Vol. 32, No. 11, pp. 1492-1513.

Walters, G. (2001) ‘Privacy and security: An ethical analysis’, *Computers and Society*, Vol. 31, No. 2, pp. 8-23.