

# Privacy in the Context of Digital Social Environments: A cyber-Sociological Perspective<sup>1</sup>

Thierry Nabeth

INSEAD, CALT (the Centre for Advanced Learning Technologies),  
Bvd de Constance, 77305 Fontainebleau Cedex, France  
[thierry.nabeth@insead.edu](mailto:thierry.nabeth@insead.edu)  
<http://www.calt.insead.edu/>

**Abstract.** The Internet is increasingly being employed as a means to facilitate the social process of human communities, and in particular a large variety of categories environments and mechanisms (such as Email, forums, blogs, reputation systems, wikis, MMORPG, etc.) are now available to mediate people interaction. In this context, people information (declared or observed) plays an essential role, since it intervenes directly in the establishment and development of human relationships (for identifying others, for assessing trust, etc.). This paper examines and illustrates with a few examples, the concept of privacy in the context of social digital environments. It indicates in particular the difficulty to manage and protect a category of information that people are encouraged to disclose in order to fully benefit from these systems or that many people are not really aware of.

## 1 Introduction

The Internet is increasingly becoming more alive and more social, moving away from the idea of Internet as only a gigantic encyclopedia or a massive shop, and in which the interactions only happen with machines. People today not only use the Internet more and more to interact others people, but they use it to socialize, to generate some lasting relationships, and even to develop a “real” social virtual life (in online forums, chats, massively multi-player online games, etc.).

In this context, the online identity that people develop represents a critical element of the activities taking place in these virtual spaces. This digital identity - that represents how they are perceived in the online environment -, has a direct impact in enabling or preventing the social interaction, and on the nature of the interaction. For instance you do not interact the same way with someone that you know and you trust than with someone for whom you have no information at all. This online identity can be explicit, and managed by some sort of identity management systems, or can be more abstract and diffuse. In the latter case, it includes the social identity that people

---

<sup>1</sup> This paper was produced as part of the Network of Excellence FIDIS (Future of the Identity in the Information Society), a project of the 6th Framework programme of the European Commission

develop on line and that exists in the form of the reputation that they acquire (in forum, blogs, etc.) or the network of relationships that they build (in "friends" specified in their blogs, in the Instant messaging buddy list, etc.) or in the form of their contributions in the public spaces (posting in bulletin boards, etc.) or in the digital traces that they leave and that are recorded in log files.

The existence of this identity that people are encouraged to develop (so as to maximize the benefit they get in using these environments) raises a certain number of privacy issues. The first problem is related to the underestimation of the quantity and the nature of the information that is captured in these systems. People are for instance not fully aware to which level their behavior can potentially be tracked when they are online, nor do they perceive the real usage that can be done of this information. The second problem is related to the false sense of security that people develop when using systems that are easy to utilize. For instance blogging or peer-to-peer network are very user-friendly, but in reality they can easily conduct their authors to actions for which they overlook the consequences (such as disclosing confidential information, breaking some laws and revealing more information about themselves than what they intended to). Another problem comes from the persistency of the information that is digitally captured, and that can later result in unpredicted consequences long time after. For instance people disclosing too easily their email address take the risk of having this address exploited by spammers for years. People having posted some opinion on a bulletin board take the risk of having this information discovered after a very long amount of time.

The objective of this document is to present an overview of digital social environments from the viewpoint of the subject of privacy. Its aim is to raise awareness on the diversity and richness of these environments, on the different privacy issues that may happen in these environments, and the difficulty to address them with only pure technical solutions.

The first part of this document consists in a general presentation and analysis of the digital social environments and the problems of privacy they may raise. This document then presents the main categories of digital social environments in the viewpoint of privacy, and illustrates each of them with a case or story presenting a particular privacy issue. It then concludes by providing some directions of future thinking such as the use of education or social engineering as a way that can contribute to the elaboration of more robust solutions able to procure some level of protection of the privacy of the individuals, and at the same preserving the flexibility and the value of these environments.

## 2 The Digital Social Environments, and the Privacy Issues

### 2.1 Digital Social Environments

The increase of the social dimension on the Internet

As the Internet is becoming more mature and is being adopted by a larger (and in particularly less technophile) portion of the population, its usage is becoming less information centric, and more oriented towards the mediation of the social process. More concretely, people are increasingly using the Internet to engage in activities that include a strong social dimension such as: the participation in communities of interest (intervening in online forums and other virtual community spaces), the expression of their opinions, visions, and description of their lives etc. via personal journals that are made available to others (the “blogging phenomenon” (Kumar et al. 2004)), the exchange of opinions and the building of reputation (examples include reputation systems’ mechanisms found in eBay), the participation in online games or virtual worlds in which the players intervene as avatars, or the use of matching systems (dating systems, social networks) which are used to help the establishment of relationships with other people and to exploit them. If the social dimension of the Internet is not new (emails and newsgroups have supported the social process for years), it is however changing in nature since it is now becoming accessible to the “non-geek” population, is more deeply supported (they are no longer seen only as “side products”, and for instance social network systems aim at explicitly supporting them), and is experiencing a major revival after the new evolution of the World Wide Web as a less information-centric and a more service-oriented system (see for instance (Fox et al., 2005) for some predictions about the evolution of the Internet).

The digital social environments (DSE)

A certain number of tools, the Digital Social Environments (DSE), have been elaborated to implement this vision of a more social Internet and which aim at supporting the online social process.

We define DSE as the category of Online Environments that provide some form of support to the social process. This definition is rather broad, and includes a variety of systems ranging from very explicit and centralized community systems directly supporting people’s interactions (such as virtual community platforms or forums), to some more decentralized communication systems that are supporting a more peer-to-peer mode of interaction and that are directly controlled by their users (for instance email, Instant messaging systems, blogs). DSE also include environments that do not directly support people’s interactions themselves, but provide some services of intermediation. In a similar way these services can be centralized (for instance a system like eBay which provides some matching services between vendors and buyers, and implement a series of reputation mechanisms), or decentralized (such as

in the case of online social networking systems like LinkedIn in which people manage individually their social network, or peer-to-peer networks that are used to directly exchange digital items).

	Communication & Interaction	Intermediation
Centralized	Virtual community systems, Forums, Wiki, MMOG, CMS, etc.	Marketplaces (reputation and recommender systems), ...
Decentralized	Blogs, Instant messaging, email, etc.	Online social networking, peer-to-peer networks, etc.

Table. 1. DSEs centralization / interaction

“Table 1: DSEs centralization / interaction” summarizes this categorization of DSEs according to their centralized or decentralized nature, and on their main role (support for the interaction or intermediation), although in reality the frontier is not always very strict, and that we see some movement of convergence and merging of these systems into more holistic ones (for instance Bill Gates in (Kanellos, 2005) suggests for the future the integration of everything – social networking, blogging, instance messaging, etc.- into a single system).

## 2.2 Privacy

### Privacy issues in DSEs

These socially enhanced digital spaces bring a certain number of privacy issues that originates from the underestimation of the amount of data effectively captured and the misunderstanding of its usage, the false sense of security that the overfriendliness of these systems provide, as well as the risk associated to the persistence of the data.

In many cases, people enter into these environments using masks (pseudonyms), to engage into some activities for the fun, and in particular for the possibility to experiment with a new identity. Examples include the domain of the virtual worlds (gaming, virtual communities, virtual dating, etc) that people use for the purpose of changing for and experimenting temporarily with a more desirable life than the one they have in the real world (in other words, the value that people get from these worlds is exactly in the possibility to “pretend” to be someone else) or for alternate lives (gender switching is not uncommon). For instance, a fantasy world will give an insignificant employee in the real world the opportunity to become a renowned knight (Steinkuehler, 2004), a blog will provide a professor the possibility to become a rock and cultural critic (Nardi et al., 2004), and a dating system will permit an introvert to overcome his/her shyness in an online world and to engage in some relationships with individuals of the opposite gender.

The risk associated to the divulgation of this virtual identity can appear very limited, since it is perceived from the beginning to belong to the non-serious sphere, and of the imaginary realm than the real world. In such an environment, the misbehaving can be considered not to reflect the inner characteristic of this user, but rather as a role that was temporally adopted to play a game. Yet even in this case privacy problems can be rather annoying, and sometime ruin totally the online experience by hurting the feelings of a person in a way that is anything but virtual. For instance, in a famous case of gender switching (Van Gelder, 1991), a man was able to extract very intimate information from women by pretending to be one of them. We can easily imagine that similar things that in the future sexual maniac would be able to extract similar category of information from a group of children interacting in a chat room. We can also mention the case of several bloggers that found themselves out-of job, after their employer has discovered what they had posted, in their blog (blogs are personal online journals used to express opinions) that they once considered as personal and not to be taken too seriously.

In some other cases, people enter into these environments to conduct very serious activities in domain such as commerce, consulting, knowledge exchange, or communication. For instance independent vendors have developed commerce on eBay (an electronic marketplace providing reputation mechanisms) and depend on it for their living. These vendors rely heavily in their commerce from the different feedback that their customers leave at the end of a transaction and that help them to build a reputation. In a similar way, consulting activities are conducted in services such as eLance.com. In this case, the feedbacks are no longer concerning products but consulting missions, and therefore the person itself (the consultant in this case is often self-employed), pushing further the question on the limit between the work sphere and the private sphere. Knowledge workers are increasingly using the virtual communities of interest in which they develop important relationships with their peer, and for which the online identity and reputation they develop is increasingly important to conduct their work. Finally, activists and defenders of individual freedom are using the public spaces offered by the virtual community systems as the tool of choice to express their free speech, or defend their liberty. In these latest cases, pseudonymity offers them some level of protection from the risk of retaliation from governments, companies, fundamentalist groups, etc..

Are privacy issues really important in DSEs?

Again, it is of course legitimate to question the importance of these identities that develop in digital social environments and in particular the information attached to the virtual person: after all, these virtual worlds are not real, and the consequences can only be minor, and in no way similar to privacy issues that occur in the real world! This would be forgetting that these digital social environments are gaining an increasing importance in people's lives. For instance (Stafford and Gonier, 2004) in a study of AOL users' population report that socialization is now recognized as a significant factor for using the Internet, and a Pew Internet & American Life Project report ((Rainie, 2005) indicates that end 2004, 7% of the 120 million U.S. adults who use the Internet say they have created a blog, and 27% of Internet users say they read blogs. We can also add that the ruining of an online reputation can be disastrous in real life (when it happens for an eBay vendor or for a politician) and that the frontier

between these worlds and the real world is progressively blurring (for instance a project such as I-Neighbour helps to strengthen local bonds and social interaction by vitalizing real local communities, blended learning combining the online and off-line learning is increasingly attracting attention about the future of learning, etc.).

### 3 Illustrating Privacy Issues in Digital Social Environments

In this section, we are going to provide a more concrete overview of the different categories of the digital social environments, and for each of them, we will give an example, case or scenario illustrating a particular privacy issue.

#### 3.1 Electronic mail

Email communication represents one of the most important tools used on the Internet (Stafford and Gonier, 2004), and one of the oldest. Electronic mail represents the principle means for people on the Internet to communicate directly and asynchronously with one another, which consists in the transmission of a message to a given electronic destination of the receiver.

The Identity in email systems is essentially managed via the email addresses (identifier@domain) that people utilize to communicate with one another. Practically, people's authentication is done by the "sender" attribute in the email. Privacy is protected by the non-disclosure of this email to third parties (which may be difficult because this information may be transmitted from a party that was originally trusted). Some information can be inferred from the domain of the email address (this domain sometimes represents the name of the organization to which the user is affiliated, such as a company or a university). Electronic mail is sufficiently well known to have to further describe it in this document.

The email system raises a certain number of privacy problems. The most visible one is probably the problem of invasion of the private space by the spam: the email address that was originally considered as personal is becoming the target of the advertising of perfect strangers. A more serious thread is spoofing, which originates from the possibility to very easily forge an address and to borrow someone else (or organization) identity. Spoofing, has been used in some cases to harm the reputation of individuals or organizations by making them "say" things considered as inappropriate. Spoofing is also used to mislead the receiver, and typically to make him / her disclose some information of private nature (for instance a spoofer will pretend to be a bank in order to extract credit card information or a social security number). Another more interesting example of major disclosing personal information via email is given major Internet player Yahoo, which in exchange for a free massive mailbox, ask the right to mine the content of the emails in order to display automatic advertisements based on the text of e-mail messages (McCullagh, 2004).

### 3.2 Virtual Community Environments

Virtual community environments include all the systems, such as forums or bulletin boards, that provide explicitly shared dedicated spaces for supporting the discussions of communities or groups of people. The communication in these spaces can be asynchronous (bulletin board) or real-time synchronous (chatrooms). People interact mainly with others by posting messages in (public or restricted) share spaces, but can also sometimes communicate directly and more privately with one another. The control of what can be posted in the public spaces (specified in an explicit or implicit code of conduct) can be enforced by a moderator or by some social regulation mechanisms (typically social pressure).

The privacy issues in such environments are not “a priori” very different in nature from the ones that can be found in the off-line communities. They are just considerably magnified. Like in a small town, people behaviors can be observed, reputation can be created, and the content of conversation can be repeated. One of the main differences that comes in mind is the higher level of transparency, the more important reliability of the data and its permanence (this data can not be deformed, and it can potentially persists a very long time).

Another very important difference is related to automatic treatment of the people information: the traces that people leave in the shared spaces are accessible for automatic monitoring and analysis. For instance, some research experiments funded by intelligent agencies have been conducted to spy on the activities of chat-rooms (McCullagh, 2004b). We can easily imagine that the mining of forum can also easily be achieved, for instance to identify deviant behaviors! Finally, on a different level, we can mention the use of social psychological theories taking advantage of identity information, to manipulate the people “inhabiting” these communities (for instance (Beenen et al., 2004) investigate strategies to be activated to motivate the contributions to online communities, but we can easily imagine other manipulations aiming at far less acceptable objectives).

An interesting case of a privacy issue that we have already mentioned is related to identity phishing (someone create a false identity in order to mislead other persons). The Strange Case of the Electronic Lover (Van Gelder, 1991) tells the story of Joan Sue Green, “...a New York neuropsychologist in her late twenties, who had been severely disfigured in a car accident that was caused by a drunk driver.” The accident killed Joan’s boyfriend and left her mute and confined to a wheelchair. But, through the use of her computer and the participation in a BBS (Bulletin Board System), Joan was able to befriend many users and let her bubbly personality shine. The reality proved to be different: Joan was not a disabled person, and it appeared that Joan was a man. Under his “feminine identity”, this man was able to develop online relationship with other woman, and to extract very intimate information from conversations with them.

### 3.3 Blogging

Blogging represents the last avatar or “phenomenon” of the “Internet revolution”, and is developing at a tremendous rate (Kumar et Al, 2004). Blogs are online journals that are commonly used to chronicle the lives and opinions of their authors. Blogging provides the possibility for people to develop a personal identity that they are able to project in a social space (the bloggosphere) and to enter into interaction with their audience (visitors are invited to comment the blog postings of the owner of the blog). Blogs are also often interdependent: people frequently quote postings from other blogs and some mechanisms are provided to support this cross-referencing between blogs (for instance the trackback is used to notify automatically to another blog that it is being referenced). Besides, blogs often reference explicitly other blogs (acquaintances), creating some networks of blogs.

The management of personal information should appear to be quite simple in a blog, since blogs are totally controlled by their owners: it should be up to its owner to decide which information to make available to his/her public. The reality, however, is more complex. First, in a blog a user can reveal a great deal about himself/herself without fully perceiving the extent of this provision of information (blogging systems are very easy to use technically and posting is often impulsive, and besides the perception of the audience is not very elaborated). One of the main problems with blogging is the lack of clear separation between the private sphere and the public sphere and the risks of information leaking that can happen (for instance (Suitt, 2003) discusses a Harvard Business Review case related to personal blogging in a work context and its implications). To add to the complexity, it should be mentioned some evolution in the way that blogs are controlled. The last version of the blogging space MSN space from Microsoft is now controlled and is subject to automated censorship (MSN is considered to be liable for the content posted on the spaces no longer seen as totally private).

A particularly revealing example of the risk that blogging bring to their author is given by the case of several people that have been fired by posting company information in their “personal blog” (Metz, 2004). Concretely, a flight attendant in Texas, a temporary employee in Washington and a web designer in Utah were all fired for posting content on their blogs that their companies disapproved of. A similar story also happened recently in the UK, where an employee was fired because of what he posted on his blog (Barkham, 2005).

### 3.5 Instance Messaging (IM)

Instant messaging (IM) are real time communication systems that allow an individual to communicate immediately in real time with another user (other usages include the creation of temporary private chat-rooms supporting the instant communication of groups of individuals). Examples of Instant messaging systems include Yahoo! messenger, Windows messenger, AOL instant messenger or Exodus (used in the open source community). IM systems represent an important communication tool that is

used by millions of Internet users ((Shiu and Lenhart, 2004) indicate that 53 million adults trade instant messages and 24% of them swap IMs more frequently than email). IM identity profiles are relatively sophisticated in IM systems. They comprises an in-depth user profile describing the characteristics of this user (age, location, picture, interest, etc.) and well as a list of contacts (buddy list referencing the instant messaging acquaintances of this user). Users are also able in an interaction to use some visual tags (emoticons) to indicate mood or emotion (which can help the establishment of confidence). An interesting concept supported by IM systems is the management of presence. Practically users are able to indicate to others (and reversely receive indication from others) about their online status: if they are online or offline, busy or available for interaction, or invisible (the users are in control of the indication of their online presence).

One of the main identity issues with IM is the invasion of privacy (Saunders, 2002)). In a study (Patil and Kobsa, 2004) have identified three privacy concerns: Privacy from Non-contacts (i.e. people who are not part of the contact list), privacy regarding availability (busy/available, at home/at work, etc.) and privacy regarding content (which has to do with the sensitivity of the content of the IM conversations). The privacy regarding the content also relates to the saving of conversations and their divulgation to a third party without the consent and knowledge of one of the parties (therefore a user may have to be liable for private talks happening in an informal chitchat).

Criminal investigators are increasingly exploiting digital information to track crime. In September 2003, in the context of an investigation of security fraud, state and federal prosecutors for the first time searched IM records of licensed brokers and dealers (Smith, 2003). In that case the investigators were able find evidence in the IM traces of a former Bank of America broker which were related to the execution of after-hours mutual fund trades.

### 3.6 Online Social Networking (OSN)

Online social networking services (OSN) represented the latest avatar of the "Internet revolution" (Braunschweig, 2003) ... before the blogging phenomenon took over this "title". Socialware are services that are helping individuals to manage and develop their social relationships. Social capital represents indeed a critical element of individual performance in the knowledge economy characterized by less institutional stability and fewer reliable corporate resources (Nardi, 2000) and in which the individual has to behave more autonomously. OSN intervene in a number of domains (Li, 2004; Leonard, 2004): friendship (with friendster.com), business relationships (with LinkedIn, Ryze), jobs (Borzo, 2004), community of interest (Orkut, Tribe), etc. To some extent, we can consider that online dating services belong also to the category of OSN.

Practically, OSN are matching and intermediation services based on two elements: (1) the definition of a user profile in which people can specify their interests and affiliations (people can have this affiliation "confirmed" or endorsed by other members of the network); (2) the explicit specification of a social network of acquaintance that is built via a series of invitations to join the social network by other

members of the network. It is important to note that a member is not obliged to accept this relationship, and therefore that a relationship is always the result of an acceptance by both parties (the one that has initiated the relationship, and the one that has accepted the relationship to be established). Different services, exploiting this information and in particular the network, are then possible such as: searching for people (the results are displayed according to social proximity); intermediation (invitations can be relayed via this network from one member to another). In addition, the members have also some control on the visibility of their network for others. For instance some members can decide to make visible their social networks only to their direct acquaintances.

Online social network systems represent a fascinating field of practical application of some important social theories, and in particular the theory of the Small World or the Six degrees of separation by which on average the distance in social networks between complete strangers is less than six (Watts, 1999) or the theory related to the power of weak ties (Granovetter, 1973). It also poses some of the most critical challenges to the privacy protectors: the social networks represent some of the most personal information attached to an individual and the fact that people are ready to enter it in a computer would indicate that the any hope to protect people identity is doomed to fail. The reality is however somewhat different when you happen to know that some people enter in some context to create the online largest social network that count almost a thousand members, and bring to question the real criticality of the information that is really entered in these systems (Leonard, 2004; Kahney, 2004).

### 3.7 Reputation systems

#### Description and identity issues

Electronic commerce is no longer only seen as a very “efficient” procurement system optimizing the matching between the demand and the offer as well as the supply chain, but also as a space where the different actors (both vendors and buyers) can interact with one another. For instance, before engaging into a business transaction, customers will use the Internet to collect opinions from other customers that will help them to decide what product to buy and which vendor to choose. Electronic commerce also comprises the establishment of closer relationships between the vendors and the customers, and in particular more direct interaction: for instance the creation of a blog for commerce will allow a vendor to communicate information to its prospective clients, but also to engage in an interaction with them. Finally, electronic commerce also includes the reputation systems, popularized by eBay, and which represent electronic marketplaces enhanced with mechanisms supporting the establishment of reputation.

Practically, reputation systems are based on the gathering of comments from buyers and sellers about each other after each transaction, and about making this information visible to the whole community (Resnick et al., 2000). In a reputation system, a new prospective buyer for a product can get access to the whole history of the transaction of the vendor of the product, as well as all the comments that this vendor got from the previous buyers. Obviously bad opinions on previous transactions or the absence of

opinions (in the case of a new vendor) will raise suspicion about the seriousness of the vendor, and will seriously reduce the willingness of clients to engage in a transaction. In a similar way, a vendor has the possibility to check the reliability of a client interested by his items, and to decide to refuse to proceed with the transaction. In the latter case, indicators of unreliability of the client include the online age of this customer, the number of transactions that this customer has engaged in the past, and the opinion that this client gave to other vendors or received from them.

It is very clear that one of the main functions offered by reputation systems is the support for the establishment of an explicit online reputation of the different actors (vendors and clients) involved in an electronic marketplace. This reputation can be considered as an attribute attached to the identity of this actor, and more particularly to its social identity.

Still, reputation systems (that can also be applied outside the field of the electronic commerce) are not without raising a number of privacy issues and are at the origin of several problems. For instance, inconsiderate social transparency can in some cases have a negative effect of reinforcing conformance in (virtual) society, "punishing" deviance, and encouraging segregation. The second problem is related to reputation manipulation. For instance (Dellarocas, 2000) indicates that the rating of sellers can be unfair (intentionally false) in order to artificially raise the reputation of a vendor (as would be the case when a vendor creates false transactions just to increase his/her reputation), or decrease it (as conspiring buyers or competitors would do). In his paper, however, (Dellarocas, 2000) indicates some mechanisms to use to fight against this identity falsification. Finally, we can also raise some ethical issues: how far can social identity be managed and processed by automatic mechanisms that can impose important pressure on individuals (for instance, in the case of the eLance marketplace, in which the goods that are traded are small consulting missions).

### 3.8 Other DSEs (MMORPG, peer-to-peer network, Wikis, etc. ....)

Most of the digital systems that deal with people potentially raise some privacy issues, and all the other DSE do not make an exception. The interaction in a MMORPG (Massively Multiplayer Online Role Playing Games), the use of peer-to-peer networks (Kazza, Napsters and the likes), the contribution in a Wiki (a wiki is a web site that can be extremely easily be author by a community of people) mechanically leave traces, and reveal information about their author. In a MMORPG, this information can consist in the behavioral profile of a player (for instance his/her aggressiveness). In a peer-to-peer network, this information will consist in the preferred style of music. And in a Wikis, this information will indicate the interests of a user and his/her knowledgeability of a domain.

Managing people privacy in such diverse an complex environment represent indeed a challenge to which the solution can probably not be brought by the technology alone (people are inevitably in the loop in such systems, and the people are more foible than machines).

## 4 Discussion and Conclusion

Digital Social Environments represent a fascinating field of investigation of the privacy issues, and all identity issues in general. Indeed, it first it magnifies the traditional challenges of privacy concepts that already exists in the off-line world of the social relation (such as reputation, transparency, etc) to an extreme levels given the digital mechanism that support the social process (the examples that we have mentioned in this paper include the electronic social networking systems, the reputation systems, etc.). Even more radically when compared to the offline world, it potentially give access to a huge quantity and variety of personal information that can be the subject to automatic treatments.

Still, it would be illusory to believe that this same technology alone, and therefore purely technical solutions would be able to address all these issues, in particular in environment in which the human factors are so important, even if they can bring some benefits. Interestingly, the adequate solution could come from observing the digital criminal themselves that appear to be the more effective with only using the information technology alone, but by exploiting people credulity using some social engineering techniques.

We can imagine, and we hope that this paper and its several illustrations will have helped to clarify this, that the successful management of privacy in environments in which the social dimension is important, will be the one that will be able to combine the technology enhancing the privacy, with the less technical approaches and strategies that originate from other disciplines (such as sociology or education).

## References

1. Kumar R., Novak J., Raghavan P., Tomkins A. (2004); "Structure and evolution of blogspace"; *Communications of the ACM* 47(12): 35-39, 2004.
2. Fox Susannah, Janna Quitney Anderson and Lee Rainie (2005); "The Future of the Internet"; Pew Internet & American Life Project report; 9 January 2005
3. Kanellos Michael (2005); "Gates taking a seat in your den"; Cnet news.com, January 5, 2005 [http://news.com.com/Gates+taking+a+seat+in+your+den/2008-1041\\_3-5514121.html](http://news.com.com/Gates+taking+a+seat+in+your+den/2008-1041_3-5514121.html)
4. Steinkuehler, C. A. (2004). "Learning in massively multiplayer online games"; In Y. B. Kafai, W. A. Sandoval, N. Enyedy, A. S. Nixon, & F. Herrera (Eds.), *Proceedings of the Sixth International Conference of the Learning Sciences* (pp.521–528).Mahwah, NJ: Erlbaum
5. Nardi B., Schiano D., Gumbrecht M., Swartz L. (2004); "Why we blog"; *Communications of the ACM* 47(12): 41-46, 2004.
6. Van Gelder, Lindsay (1991); "The Strange Case of the Electronic Lover"; In *Computerization and Controversy: Value Conflicts and Social Choices*, edited by Charles Dunlop and Rob Kling, Pages 364-375
7. Stafford Thomas F. and Dennis Gonier (2004); "What Americans like about being online"; *Communications of the ACM archive*, Volume 47, Issue 11 (November 2004)
8. Rainie Lee (2005); "The state of blogging"; Pew Internet & American Life Project report, DATA MEMO, January 2005
9. McCullagh Declan (2004); "Gmail and its discontents"; CNET News.com, April 26, 2004

10. McCullagh Declan (2004b); "Security officials to spy on chat rooms"; CNET News.com, November 24, 2004
11. Beenen, Gerard, Ling, Kimberly, Wang, Xiaoqing, Chang, Klarissa, Frankowski, Dan, Resnick, Paul, and Robert E Kraut (2004). "Using Social Psychology to Motivate Contributions to Online Communities". To appear in Proceedings of ACM CSCW 2004 Conference on Computer Supported Cooperative Work, Chicago, IL. 2004
12. Suitt Halley (2003); "A Blogger in Their Midst"; Harvard Business Review, vol. 81, no. 9, September 2003
13. Metz Rachel (2004); Blogs May Be a Wealth Hazard; Wired magazine, December 6, 2004 <http://www.wired.com/news/culture/0,1284,65912,00.html>
14. Barkham Patrick (2005); "Blogger sacked for sounding off"; The Guardian, Wednesday January 12, 2005
15. Shiu Eulynn and Amanda Lenhart (2004); "How Americans Use Instant Messaging"; Pew Internet & American Life Project report, September 2004.
16. Saunders Christopher (2002); "Enterprise IM Spurs Privacy Concerns"; Instant Messaging Planet.com, November 18, 2002 <http://www.instantmessagingplanet.com/enterprise/article.php/1502941>
17. Patil, S. and A. Kobsa (2004): Instant Messaging and Privacy. Proceedings of HCI 2004, Leeds, England.
18. Smith Elliot Blair (2003); "Wall St. Bloodhounds Track IMs for Clues"; USA Today, 23 September 2003 [http://www.usatoday.com/money/companies/management/2003-09-18-ims\\_x.htm](http://www.usatoday.com/money/companies/management/2003-09-18-ims_x.htm)
19. Braunschweig Carolina (2003); "The new Internet Gamble"; Venture Capital Journal, December 2003
20. Nardi, B., Whittaker, S, Schwarz, H. (2000); "It's Not What You Know, It's Who You Know: Work in the Information Age"; First Monday, May, 2000
21. Li Charlene (2004); "Profiles: The Real Value of Social Networks"; Forrester Research, July 15, 2004
22. Borzo Jeanette (2004); "Online Social Networks Are Havens for Job Hunters"; CareerJournal.com, September 23rd, 2004 <http://www.careerjournal.com/jobhunting/networking/20040923-borzo.html>
23. Watts Duncan (1999); "Small Worlds: The Dynamics of Networks between Order and Randomness"; Princeton University Press, Princeton, 1999).
24. Granovetter Mark (1973); "The Strength of Weak Ties"; The American Journal of Sociology, 78 (May): 1360-1380, 1973
25. Leonard Andrew (2004); "You are who you know"; Salon.com, June 15, 2004 [http://www.salon.com/tech/feature/2004/06/15/social\\_software\\_one/](http://www.salon.com/tech/feature/2004/06/15/social_software_one/)
26. Kahney Leander (2004), "Social Nets Not Making Friends", Wired magazine, Jan. 28, 2004
27. Resnick, Paul, Richard Zeckhauser, Eric Friedman and Ko Kuwabara (2000); "Reputation Systems: Facilitating Trust in Internet Interactions"; Communications of the ACM, 43(12), December 2000
28. Resnick, P., R. Zeckhauser, J. Swanson, and K. Lockwood (2002); "The Value of Reputation on eBay: A Controlled Experiment," U. of Michigan Working paper, originally presented at the ESA conference, June 2002
29. Dellarocas, Chrysanthos (2000); "Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior"; Proceedings of the 2nd ACM Conference on Electronic Commerce, October 2000