

Peer Reviewed Article

Vol.8(2) June 2006



Slave or sibling: a moral reframing the corporate knowledge sharing community

J.C. du Plessis

School of Information Studies University of Wisconsin-Milwaukee Milwaukee, USA

J.J. Britz

School of Information Studies
University of Wisconsin-Milwaukee &
Department of Information Science
University of Pretoria
Pretoria, South Africa
britz@sois.uwm.edu

R. Davel

Department of Information Science University of Pretoria Pretoria, South Africa

Content

- 1. Introduction
- 2. Sharing of knowledge and information
- 3. To share or not to share...
 - 3.1 Reasons for resisting collaboration and the exchange of knowledge
 - 3.2 Reframing the context of knowledge sharing
 - 3.3 Trust as a central moral notion in the sharing of knowledge
 - 3.4 Trust and the sharing of knowledge
 - 3.5 Responsibility and accountability
 - 3.6 Knowledge sharing environment
 - 3.7 Accessibility and security
 - 3.8 Honesty and deception
 - 3.9 Caution, harm and censorship
 - 3.10 Corporate social responsibility
- 4. Ethical principles
 - 4.1 Principle of justice
 - 4.2 Justice and knowledge creation and sharing
 - 4.3 Justice and fair compensation
 - 4.4 Justice and fair protection and retribution
 - 4.5 Justice and recognition of human dignity and autonomy
- 5. Conclusion
- 6. References

Key words: Knowledge sharing, ethics, knowledge creation, justice

'The only thing to do with good advice is pass it on. It is never any use to oneself' Oscar Wilde (1854–1900)

1 Introduction

Within the modern global economy, market places are continuously subjected to change. These changes diminish the period for which organizations can hang on to a specific competitive advantage. Owing to the fact that knowledge can be regarded as their most competitive product (internally as well as externally), organizations encourage the creation of new knowledge and exploit their existing knowledge in order to leverage their competitive edge.

To capitalize on their *knowledge pool*, organizations should therefore promote the sharing of knowledge, not only internally between employees but also externally between their employees and their customers, partners and shareholders. However, it is important that knowledge be shared in an ethical manner.

According to Wade (2002:2), ethics is concerned with 'the rightness and wrongness of human behavior including accountability and responsibility' while Gert (cited in Resnik 1993) maintains that ethics is 'a system of public, general rules for guiding human conduct'.

Ethics can therefore be regarded as a discipline dealing with good and bad, which influences people's decisions as well as their judgments on the actions of others as well as their own and involves an underlying conviction and a moral obligation of doing what is regarded as 'right' (De Jager 2002:82).

The purpose of this research was to investigate the different ethical issues pertaining to knowledge sharing within organizations and how to create an ethical atmosphere conducive to knowledge sharing by a reframing of the employee's context.

In this article, the different ways in which knowledge can be shared within organizations are briefly examined, followed by a discussion on the various ethical challenges related to knowledge sharing within organizations. Following from this, ethical principles based on justice as a moral tool within companies are discussed. The authors consider the benefits of knowledge sharing in a corporate environment and explore the reasons why sharing often does not happen. The discussion then centres on trust and the authors present a framework built around the principles of justice to nurture a knowledge sharing environment.

2 Sharing of knowledge and information

Although the emphasis of this article is neither to explore the semantic reach of knowledge as a concept, nor to evaluate the theoretical correctness of knowledge transfer as a concept, the authors wish to state their view briefly on the usage of the terms *knowledge* and *information* and the concept of *transfer*. They do so to create a common frame of reference, so that the reader can better relate to the expressed views.

In communication it is only data that are transferred. The frame of reference of the receiver of communication depends on a common understanding of the code exchanged between sender and receiver. This enables the receiver to see the information in the data. Information is seemingly transferred, yet this transfer is built upon the ability of the receiver to reconstruct the meaning represented by the data received as they express the intent of the sender. At a higher lever, the same can be said for knowledge. In essence, knowledge is constructed from various activities, which includes

tor

reasoning, reflection, hands-on trial-and-error efforts, the show and tell of others and from understanding that is gained from listening and reading. The communicative act then anticipates the reconstruction of information from data, and the dynamic development of knowledge that includes the sharing of experience, understanding and factual information.

Within organizations knowledge and information can be shared in a personal interactive manner, for example in mentorship programmes; video conferences; internal conferences; discussion forums; chat rooms; best practice networks; communities of practice and e-mail. Indirect sharing could happen within intranets; document sharing systems; collaboration tools such as Lotus Notes and through decision support systems.

top

3 To share or not to share...

An essential question that highlights the issue is: Why does sharing matter? According to Wade (2002:1–2), knowledge often increases when shared with others. In the competitive environment in which organizations interact today, the creation and application of new knowledge are vital to their survival. Reasons why organizations would benefit by knowledge sharing include the retaining of intellectual capital, empowering members to make more knowledgeable decisions, to leverage expertise learnt and applied in one part of the organization in other areas and the fact that the knowledge base of organizations is continuously eroding (Gurteen 1999).

Research by Michaelson, Watson and Black (1989) provides compelling evidence that collaboration and sharing outperform the efforts of the best non-sharing individual consistently. In this study, students took tests throughout a semester. After the completion of the individual test, each group discussed each question and decided upon an answer that represented the group consensus. In a consistent manner, the group outperformed the best individual by at least 12 percentage points. This seems to indicate that the choice between collaboration and group thinking versus relying on individual efforts consistently favours the collaborative option. The key challenge is how to structure the framework within an organization to promote the sharing, exchange and collective building of intellectual capital.

3.1 Reasons for resisting collaboration and the exchange of knowledge

There are legitimate reasons, for example privacy and security, that discourage or forbid the sharing of certain types of knowledge within organizations. For example, to prevent alarm and panic, certain information might not be publicly announced. It may also be considered unethical to share passwords and accounts to databases with other members within the organization, if access rules to these databases indicate that only one password per person is allowed (Hannabus 1998:93). A professional code of ethics is therefore needed to decide when to share and with whom to share certain knowledge within organizations.

In a setting where the sharing of knowledge might be seen as advantageous, there might still be some hindrances to achieving the objective. With the mindset that 'knowledge is power' individuals are often predisposed to be reluctant in sharing their knowledge for fear of losing their competitive edge. Wade (2002:8) describes the deliberate withholding of knowledge from staff members as 'horizontal bullying'.

Another reason why members of an organization might hesitate to share their expertise is because they either do not believe that their knowledge is relevant or they simply do not want to bring attention to themselves (Levin, Cross, Abrams and Lesser 2002:6). This, together with insecurity, lack of respect and being bad team players, might be some of the reasons why knowledge is not shared within organizations.

Within any organization there exist correlations between what people know and the structures of political power and influence. According to Hannabus (1998:92), ethical dilemmas relating to knowledge sharing within organizations are increasing. Ethics are built on elements such as trust and honesty; accountability and credit; privacy and confidentiality as well as responsibility. When applying these elements to knowledge sharing within organizations, certain ethical dilemmas may arise.

Depending on how the context is framed, the same people with the same intellectual capital would respond differently because of the particular ethical ambience the context presents.

The emphasis on the sharing of knowledge within corporations today is in sharp contrast to the older bureaucratic attitude of 'need to know' that set the political boundaries in an organization (Schmidt 2000:128).

3.2 Reframing the context of knowledge sharing

The following example illustrates how the same people in the same place saw things very differently because of how the context was framed. At the start of the French Revolution, a French officer was given the order to march his troops to a certain location of unrest in the streets of Paris and to execute the *canaille* (riff-raff). The officer marched his troops to the location and, as he feared, he found the rowdy protesters at the given location. He then proceeded to address the crowd and with great respect he addressed them as ladies and gentlemen. He then told them of his orders to execute alleged riff-raff at this location. He then kindly asked these ladies and gentlemen to step aside so that he could better identify the riff-raff that he was ordered to shoot. The crowd all stepped aside and there were no riff-raff left to shoot and he returned his troops without shooting at a single person in the street.

As mentioned above, there might be personal reasons for not wanting to step forward to share knowledge. Often talented individuals do not step forward because of how the environment has been framed. The term 'slave or sibling' illustrates the point. Tönnies (1957) identified the two terms *Gemeinschaft* and *Gesellschaft*. Within this contextual frame of reference the slave or sibling mentality is identified. The concept of a *Gemeinschaft* is to build a community with commitment and permanence. The people are there for each other, like family, for example. In a *Gesellschaft* on the other hand people are together because of a short-term objective and this alone binds these people to each other. People standing in a queue to buy football tickets might be an example. With the tickets in hand, there are no compelling reasons to keep contact with the others of the *Gesellschaft*. In this context, the term 'slaves' is used to frame workers' objects, as tools with which to achieve objectives. Siblings, however, are seen as valued individuals. There is a sense of investment in them as individuals. Within the framework of a *Gemeinschaft* there is a long-term human-centred focus, whereas the *Gesellschaft* often has a short-term objective-centred focus.

In a company, this division between *Gemeinschaft* and *Gesellschaft* happens as well. The perception (real or imagined) of the division between the *Gemeinschaft* (the siblings) and the *Gesellschaft* (the slaves or the disposables) profoundly influences the ethical ambiance. This in turn encourages or discourages participation and collaboration. The vital task that today's corporation faces is how trust can be nurtured to promote an ethical ambiance of belonging, where the individual is recognized and valued.

3.3 Trust as a central moral notion in the sharing of knowledge

The notion that trust is central in the moral reasoning regarding knowledge creation, sharing and use is well understood universally. Although a variety of classification schemes and definitions of trust can be found in the literature, the authors preferred the definition by Fukuyama who says that 'trust is the expectation that arises, within a community of regular, honest, and cooperative behavior, based on commonly shared norms, on the part of other members of that community' (Fukuyama 1995:26).

As a social and moral notion, trust is therefore closely associated with human relationships dealing with risk, change, uncertainty, cooperation, vulnerability, assistance, dependency, control and confidence. These relationships are based on the sharing of norms, values and ethical principles. Trust can therefore indeed be translated as 'normative trust' and these shared norms and values are created through the network of human relationships and form the moral foundation of social capital. Normative trust, then, manifests itself through this social capital into intellectual capital (Huotari and Livonen 2004:11).

However, the locus of trust is not in the organization itself, but resides in and between individuals. People's behavioural patterns form the basis for trust in an organization. It is therefore a moral imperative that those responsible for the sharing of knowledge in an organization must devote much of

their time to create an atmosphere in which individuals can learn to trust one another. Trust develops and grows through constant interaction and Huotari and Livonen (2004:10) point out that trust has the ability to produce more trust. It is more likely to develop trust within the context of a *Gemeinschaft* than a *Gesellschaft*.

It is also important to comment on the use of communication technologies and the building of trust in knowledge sharing. The trustworthiness and reliability of the technology systems that are used for communicating and sharing knowledge, for example the use of encryption, virus protection and authentication software, are of extreme importance. However, these applications are more concerned with security and as such do not constitute trust, but rather enable trust in the sharing of information and knowledge.

3.4 Trust and the sharing of knowledge

Not the presence of strong attachments, but sincere trust leads to effective knowledge sharing. Two categories of trust can be distinguished. The first category is a benevolence-based trust and the second is a competence-based trust. Benevolence-based trust implies that members of an organization will not intentionally harm one another when sharing knowledge. Competence-based trust, however, relies on a belief that someone is knowledgeable about a given subject area. According to a study done by Levin *et al.* (2002), knowledge sharing within organizations is more successful if the knowledge recipient regards the knowledge source as being both benevolent and competent.

The type of trust required depends on the type of knowledge that is shared. Straightforward knowledge (e.g. how to operate a microwave oven) requires less competence-based trust in the knowledge source, than when more experiential knowledge is needed, for example where to invest a large amount of money (Levin *et al.* 2002:3).

According to Skyrme (1998), there exists reluctance within organizations to share certain categories of knowledge, mainly due to a lack of trust. When people share their knowledge they need to know that it will be used appropriately, that the recipient will not take credit for it and that they will be rewarded by their organization for contributing to the corporate virtue. Only when organizational members trust one another, can useful knowledge sharing take place.

When someone has invested significant time and energy into building a relationship with an important client, he or she might be skeptic to share knowledge and information about that client with other persons or divisions in the organization. A medical agent for Johnson & Johnson, who established a firm relationship with an important hospital, might hesitate to share the details of his contacts with his colleagues, fearing that they might damage or jeopardize this relationship. For him to share this knowledge, he has to trust his colleagues implicitly. Benevolence-based trust is needed, implying that they will not try and lure his business away, and competence-based trust, meaning that in the event of his ill health a competent and knowledgeable colleague could stand in for him without harming the relationship with the client in any way.

3.5 Responsibility and accountability

Responsibility, which is normally associated with accountability and answerability to our deeds, is crucial when sharing knowledge. Responsibility and accountability implies a relationship of trust between people. It is furthermore linked to a set of shared values within an organization on which responsibility and accountability is based and judged. If people were kept accountable for the knowledge they share, they would heed, based on these shared company values, against committing fraud and carelessness.

Members of an organization tend to be more responsible when sharing knowledge with their colleagues if they are held accountable for the knowledge they share. Consequently, it is important for members of an organization to maintain high professional standards when providing knowledge, that is, providing up-to-date knowledge, using their training effectively and paying attention to specific and sensitive issues.

Three levels of responsibility regarding the sharing of knowledge in an organization can be distinguished (Britz and De Villiers 2003). They are the following:

- Functional responsibility. This level of responsibility is mainly applicable to the use of communication technologies to transfer knowledge. Knowledge should be communicated in an effective and reliable manner. This is a responsibility assigned to IT professionals and their main obligation is to see that the knowledge is being effectively and reliable communicated via technology. There is therefore no responsibility regarding the actual content and use of the knowledge that is communicated.
- Legal responsibility. This level of responsibility applies to what the law requires regarding the creation, sharing and use of knowledge. Legal responsibility is therefore mainly applicable to those who create, share and use knowledge in an organization. Based on legal responsibility, employees can, for example, be held responsible and accountable for intellectual property theft, illegal access and use of private or secret information or willfully harming others by means of defamation or other harmful information.
- Moral responsibility. This third level of responsibility protects a broader spectrum of interest and is based on a set of shared moral values in an organization to which workers adhere. Shared values that are applicable to knowledge creation, sharing and use include mutual trust, honesty, openness and sharing of a common interest between all. Even though some people enjoy sharing knowledge, the value of recognition and respect must never be underestimated (Resnik 2000). Based on this level of responsibility, workers have the moral obligation to share trustworthy knowledge with one another and not to purposefully withhold information from one another. When knowledge is shared within organizations, it is also vital, based on a moral obligation, to acknowledge those who are willing to share. Simultaneously, it is also necessary to punish when called for, for example in the event of plagiarism or the stealing of ideas. If there is no punishment for stolen or misused knowledge, members within organizations will refrain from sharing their knowledge.

3.6 Knowledge sharing environment

If organizations expect their members to share their knowledge, they have to create an environment enabling people to determine if their colleagues are both knowledgeable and willing to extend their knowledge (Levin *et al.* 2002:8). Members of an organization should be allowed to pursue new ideas and criticize old ones. Such an environment will promote the search for knowledge and truth. To foster a knowledge-sharing culture within an organization, members should be encouraged to share their knowledge, experience, methods and theories (Resnik 1993).

Often knowledge workers are forced to work under pressure and have to share knowledge quickly. Should the knowledge shared prove to be inaccurate, this could lead to mistrust among colleagues or cause people not to share their knowledge in future (Hannabuss 1998:98).

It is therefore the responsibility of organizations to create a productive atmosphere where knowledge sharing is promoted between members of the organization. Many organizations implement knowledge management tools and programs to promote internal as well as external knowledge sharing. The effective implementation and use of communities of practice can contribute to the creation of a knowledge-sharing environment.

3.7 Accessibility and security

To share knowledge effectively within organizations, it is important that members have access to knowledgeable co-workers, or document sharing systems. If members within an organization do not have opportunities to learn (e.g. through mentorship programmes or by making use of knowledge-sharing tools), they will not do it.

Sharing of knowledge and the ability to learn does not imply access to 'all information for everyone'. Certain restrictions must apply, not only to protect privacy, but also economic interests. System security is therefore an imperative and should provide the necessary barrier to prevent casual breach of ethics and to protect data from unauthorized use. Having the most elementary security procedures in place can

prevent members of an organization to access information that they have no mandate for, whether accessed out of curiosity or with malicious intent.

Sometimes a solutions provider company delivers services to rival customers. Should this be the case, the solutions provider could agree to build 'Chinese walls' between their different customer accounts. Accordingly, people within the same organization know about one another but cannot access or exchange any knowledge that might compromise the company's commitment to customer confidentiality.

3.8 Honesty and deception

Honesty is fundamental to ensure accurate knowledge sharing between members of an organization. It is important to be trustworthy, fair and forthright when sharing knowledge within an organization. Reskin (1993) argues that if knowledge is conceived or misrepresented when shared, a violation of trust takes place, causing people to refrain from sharing knowledge in future.

If people are dishonest when sharing their knowledge with colleagues, it will impact on their reputation and might cause their colleagues to either refrain from sharing all or some of their knowledge. It will also quickly lead to branding colleagues as 'reliable' or 'un-reliable' when it comes to knowledge sharing.

According to Hannabus (1998:94), ethical dilemmas with regard to honesty might arise, for example where a medical doctor refrains from informing his or her patient that he or she has a serious illness – seemingly 'for their own good'.

An example of deception can be cited from an article in the *Los Angeles Times*, on Jan Hendrick Schon, a scientist with expertise in superconductivity and molecular scale electronics, who was fired from Bell Labs for falsifying data over a four-year period. Apart from his losing a job, his actions of fabricating information also had a negative effect on the reputation of Bell Labs, whose researchers have won six Nobel prizes in physics since the organization's origin (Malone 2002).

3.9 Caution, harm and censorship

When sharing knowledge within an organization, members should strive to avoid careless errors and oversights. It is important to take note of what type of knowledge is shared and with whom. Sometimes the sharing of knowledge is restrained on the grounds that it might cause harm to the organization. Hannabus (1998:96) refers to these restrictions as 'censorship'. He argues that this form of censorship should be implemented based on the argument that people are sometimes better off if they are protected from knowing things that could be harmful.

In the same way 'organizational censorship' can also be implemented in an unethical manner, for example in the case of Gencor, an asbestos mining company in South Africa, where management knew the danger and health hazards caused by working with asbestos, or even living close to asbestos mines, and yet this knowledge was withheld from their workers. As a consequence, the company shareholders benefited greatly, while most of their workers as well as people living close to their asbestos mines started to suffer from lung-related diseases. Following class action law suits, Gencor's reputation was seriously damaged and the company had to compensate those who suffered as a result of the company's actions.

3.10 Corporate social responsibility

According to Kilcullen and Kooistra (1999:158–159), corporate social responsibility can be defined as 'the degree of moral obligation that may be ascribed to corporations beyond simple obedience to the laws of the state'. Corporate social responsibility is very closely linked to business ethics – rules guiding business practices to reflect interest in members of an organization while pursuing profits. Organizations cannot function without any moral restraints and are obliged not to inflict damage or injury to others.

It is important for organizations to maintain public as well as corporate trust and respect. Corporate social responsibility is closely related to the long-term advantages of socially responsible behaviour such as increased customer and employee loyalty and a more supportive external environment (Kilcullen and Kooistra 1999:159).

Part of the social responsibility of companies relates to the withholding of knowledge to the public. Hannabus (1998) points out that a company has, for example, the moral and legal obligation to refuse to provide knowledge or information if it has reason to believe that it will be used in a harmful way. Not making knowledge available on the method of mixing a deadly poison to the public serves as a good example of this kind of responsibility.

Another ethical issue relates to the question of when to make 'secret' knowledge of a company public. Members of an organization are normally not allowed to make confidential company information public. Employees have duties and responsibilities to their employer, but equally they have duties and responsibilities to the larger community. For example, Jeffrey Wigand, the head of research at a tobacco company, Brown & Williamson, blew the whistle when he discovered that the company was adding a certain chemical to their product, making people more prone to addiction of tobacco. He revealed this knowledge at the expense of his livelihood, reputation and family. His disclosures ultimately led to lawsuits being filed against the industry and settlements of \$246 billion (Brenner 1996).

A recent South African example can be cited where the grocery chain store Pick 'n Pay issued a warning to the public that some of its products might have been tampered with which could result in possible cyanide poisonings (Bolin 2003). Rather than keeping this knowledge private and protecting its economic interests, Pick 'n Pay behaved ethically and informed the greater community of the possible danger, thereby facing the consequences of loosing some of its customers for a certain period.

Conflict of interests between 'morality' and 'making money' might also arise when knowledge needs to be shared between companies and the public. It is generally assumed that it is the duty of an organization not to cause harm or injury to the public, yet, in adhering thereto, this could clash with shareholder interests for profits arising from the successful development and marketing of a product. For example, mobile service providers in South Africa such as MTN, Cell C and Vodacom construct cellular bay stations in order to provide a wider cellular coverage to their subscribers. However, there are rumors (not yet proven) that these bay stations cause radiation that could be harmful. The question arises, if proven harmful, should the public be informed (the ethical decision) or not (whereby the organization shareholders will benefit).

From the above, one can presume that many ethical challenges do arise when sharing knowledge within organizations. To effectively address the moral complexities, the core moral imperatives regarding knowledge management in an organization relates to:

- building of trust
- responsibility and accountability
- openness, but also respect for privacy and economic interest
- truth and honesty
- avoidance of doing harm
- recognition of human dignity.

4 Ethical principles

4.1 Principle of justice

It has been argued thus far that trust is based upon commonly shared values and norms. One of these values is justice and the reason for choosing justice as a shared value that underpins trust in knowledge sharing is fundamental to its definition: to give a person or a group what they deserve. Justice prevents harm in an organization and claims treatment that respects the humanity of employees and ensures that organizations and individuals adhere to their moral responsibilities regarding the creation, sharing and

top

using of knowledge. As a moral tool it provides the moral standard for assessing the challenges regarding the management of the knowledge within an organization.

Based on John Rawls's view on justice (1971), it is possible to distinguish the following core principles of justice:

- All employees are of equal value and should be treated as such.
- An employee ought to get what is due to he or him. This can differ from individual to individual and from context to context.
- Although all employees are of equal value, justice also recognizes the inequalities between employees in certain instances. These inequalities must nevertheless not be at the expense of the equal value of all.

Based on justice, the authors suggest the ethical principles below that can be used in moral decision making regarding knowledge sharing.

4.2 Justice and knowledge creation and sharing

Based on contributive justice, it is argued that employees have a moral obligation not only to be productive (more specifically regarding the creation of knowledge) in an organization but also to share the knowledge that benefits the organization and contribute to the intellectual commons. At the same token, however, contributive justice implies that organizations also have a moral responsibility to create an atmosphere were knowledge workers can be productive and have the opportunity to not only create, but also share their knowledge and learn from one another.

4.3 Justice and fair compensation

Knowledge creators as well as those who share knowledge must be compensated in a fair and just manner. However, it does not necessarily imply equal compensation to all. In recognizing the principle of merit, justice allows different compensation to different individuals. For example, some might create and/or share more valuable knowledge than others and compensation should reflect this difference. Compensation should also not be limited to financial incentives only. Davenport and Prusak (1998) suggest, for example, some form of official recognition of someone in the company as an expert in a certain field. Justice also requires that original creators of knowledge should have a fair share in those cases where commercial gain for the organization stemmed from their contributions.

4.4 Justice and fair protection and retribution

In focusing on the social control of harm to the organization, justice also implies some form of retribution and enforcement when it comes to the creation, sharing and using of knowledge in an organization. Those who violate the organization's accepted values and the clear articulation of what constitutes non-conforming behaviour regarding the creation, sharing and utilizing of knowledge should be fairly punished.

Among other things this would imply that legal mechanisms should be in place to appropriately protect the moral and economic interests of an organization's body of knowledge. This is specifically applicable to trade secrets and other sensitive information. In the building of trust relationships, it is also important to provide some form of legal and other forms of redress in cases where one of the parties fails to carry out its responsibility in building trust relationships.

4.5 Justice and recognition of human dignity and autonomy

Fundamental to any theory of justice and its application to various situations is the recognition of human dignity and autonomy. This normally translates into the recognition and protection of human rights. Miller points out that a 'central element in any theory of justice will be an account of basic rights of citizens' (1999:13).

Based on the discussion in this article the authors propose the following five knowledge-related human

rights:

- The right to life. As an individual and social right it includes the right to security and safety and is specifically applicable to the responsibility of organizations to make known information that can harm society. This right is also closely associated with the right to know.
- The right to the freedom of expression of ideas. This right correlates with the obligations of knowledge workers to create knowledge as well as the duty of organizations to create an atmosphere which is conducive to knowledge creation.
- The right of access to those ideas. This right correlates with the responsibility of knowledge workers to share their ideas with colleagues.
- The right to protect and control expressed ideas. This right affirms the right of knowledge creators to be fairly compensated for their work as well as the obligation of organizations to fairly protect their economic as well as moral interests.
- The right to privacy recognizes the autonomy and dignity of both employees and clients. As a right it is an expression of respect for personal and private information of people and restrict the distribution, use and sharing of private information.

These knowledge-based rights can be used as a foundation for the code of ethics in the management of knowledge in companies.

5 Conclusion

The perception within the corporate community of how the corporate environment has been framed or reframed will greatly effect the commitment and interest from individuals to be team players. Is it possible to centre the collaboration and the trust-building on a *Gemeinschaft* rather than a *Gesellschaft*? The measure of success in promoting the sharing and collective growth of intellectual capital comes from a fundamental commitment from people to invest in people. To succeed as a community, people have to foster trust between individuals, which translates into trust between groups and larger entities. If the trust between people is anchored and nurtured, then each team player will realize that there is a face behind an action, that it is someone's integrity that determines decisions and that individuals will live up to the trust they are given. This trust establishes an ethical environment that enables a collective knowledge building process to flourish so that the corporation can remain a dynamic problem solving entity for meeting the company objectives. In such an environment the principle of justice is an effective moral tool to bridge the challenges of moral complexities so that the compelling benefits of a collaborative culture can be materialized.

6 References

Bolin, L. 2003. Pick 'n Pay confirms cyanide. *News24* 1 July 2003. [Online]. Available WWW: http://www.news24.com/News24/South_Africa/News/0,,2-7-1442_1381118,00.html (Accessed 13 September 2003).

Brenner, M. 1996. *The man who knew too much*. [Online]. Available WWW: http://www.jeffreywigand.com (Accessed 29 July 2003).

Britz, J.J. and De Villiers, D.E. 2003. 'n Christelik etiese kommentaar op die morele verantwoordelikheid van Internetdiensverskaffers. [A Christian ethical commentary on the moral responsibility of Internet service providers]. *Verbum et Ecclesia* (Dec):333-358.

De Jager, P. 2002. Ethics: good, evil, and moral duty. *The Information Management Journal* (September/October):82-85.

Fukuyama, F. 1995. Trust: the social virtues and the creation of prosperity. New York: The Free Press.

Gurteen, D. 1999. Creating a knowledge sharing culture. *Knowledge Management Magazine* 2(5) [Online]. Available WWW:

http://www.gurteen.com/gurteen/gurteen.nsf/0/FD35af9606901ck2802567c70068cbf5/ (Accessed 12 February 2003).

Hannabuss, S. 1998. Information ethics: a contemporary challenge for professionals and the community. *Library Review* 47(2):91-98.

Huotari, M. and Livonen, M. 2004. Managing knowledge based organizations through trust. In Huotari, M. and Livonen, M. (Eds). *Trust in knowledge management and systems in organizations*. London: Idea Group: 1-29.

Kilcullen, M. and Kooistra, J.O. 1999. At least do no harm: sources on the changing role of business ethics and corporate social responsibility. *References Services Review* 27(2):158-178.

Levin, D.Z., Cross, R., Abrams, L.C. and Lesser, E.L. 2002. Trust and knowledge sharing: a critical combination. *IBM Institute for Knowledge-Based Organizations* 1-9. [Online]. Available WWW: http://www.ibm.com/services/insights/ibv-trustandknow.htm (Accessed 7 March 2003).

Malone, M.S. 2002. The lying game. *ABCNews*. [Online]. Available WWW: http://abcnews.go.com/sections/business/SiliconInsider_0201001.html (Accessed 7 March 2003).

Michaelson, L.K., Watson, W.E. and Black, R.H. 1989. A realistic test of individual versus group consensus decision-making. *Journal of Applied Psychology* 74:834-839.

Miller, D. 1999. *Principles of justice*. London: Harvard University Press.

Rawls, J. 1971. A theory of justice. Oxford: Oxford University Press.

Resnik, D. 1993. Philosophical foundations of scientific ethics. [Online]. Available WWW: http://www.physics.emich.edu/mthomsen/resn1.htm (Accessed 7 March 2003).

Resnik, D. 2000. Introduction to knowledge management and the DoD. *The MSIAC'S M & S Journal Online*. Spring 2000, 3(4). [Online]. Available WWW: http://www.msiac.dmso.mil/journal/sp0013/know13.html (Accessed 12 February 2003).

Schmidt, D.P. 2000. Ethics for knowledge management. In Srikantaiah, T.K. and Koenig, M.E.D. (Eds). *Knowledge management for the information professional*. New Jersey: Information Today, Inc.: 115-130.

Skyrme, D.J. 1998. Virtual trust: a key ingredient of successful knowledge sharing. *I3 Update* (19). [Online]. Available WWW: http://www.skyrme.com/updates/u19.htm (Accessed 6 March 2003).

Tönnies, F. 1957. Community and society. East Lansing: The Michigan State University Press.

Wade, R. 2002. *Knowledge management from a school experience: an ethical perspective*. [Online]. Available WWW: http://www.edfac.unimelb.edu.au/EPM/COLL/EdKM2002/WadePaper.pdf (Accessed 7 March 2003).

Disclaimer

Articles published in SAJIM are the opinions of the authors and do not necessarily reflect the opinion of the Editor, Board, Publisher, Webmaster or the Rand Afrikaans University. The user hereby waives any claim he/she/they may have or acquire against the publisher, its suppliers, licensees and sub licensees and indemnifies all said persons from any claims, lawsuits, proceedings, costs, special,

incidental, consequential or indirect damages, including damages for loss of profits, loss of business or downtime arising out of or relating to the user's use of the Website.

Published by <u>InterWord Communications</u> for Department of Information and Knowledge Management, University of Johannesburg

ISSN 1560-683X