Togetherness and Respect - Ethical Concerns of Privacy in Global Web Societies

Gordana Dodig-Crnkovic and Virginia Horniak

Department of Computer Science and Engineering
Mälardalen University
Västerås, Sweden
gordana.dodig-crnkovic@mdh.se
vhk99001@student.mdh.se

Abstract Today's computer network technologies are sociologically founded on hunter-gatherer principles; common users may be possible subjects of surveillance and sophisticated Internet-based attacks are almost impossible to prevent. At the same time, information and communication technology, ICT offers the technical possibility of embedded privacy protection. Making technology *legitimate by design* is a part of the *intentional design for democracy*. This means incorporating options for socially acceptable behaviour in technical systems, and making the basic principles of privacy protection, rights and responsibilities, transparent to the user. The current global *e-polis* already has, by means of different technologies, *de facto* built-in policies that define the level of user-privacy protection. That which remains is to make their ethical implications explicit and understandable to citizens of the global village through interdisciplinary disclosive ethical methods, and to make them correspond to the high ethical norms that support *trust,* the essential precondition of any socialization. The good news is that research along these lines is already in progress. Hopefully, this will result in a future standard approach to the privacy of network communications.

Keywords Privacy, Cyberethics, *E-polis* ethics, Legitimate by design, Disclosive ethics, Intentional design for democracy.

Technology and Culture - ICT and a New Renaissance

"The futures are out there in the setting of a coastline before someone goes out there to discover it. (...) The futures have yet to be built by us. We do have choices." (Cooley 1999 as cited in Gill 2002).

The industrial-technological era was characterized by the ideal of the perfect machine and "objective knowledge" reduced to an algorithm for constructing a "theory of everything" (Hilbert's program), with strict division of labour within different fields of endeavour. Each of the sciences was searching for its own specific and certain truths.

The post-industrial age has, however, abandoned the rigid mechanical model of a monolithic, deterministically controlled system with "the one right way" and one

absolute truth. On the contrary: it has embraced the fact that social cohesion through pluralism and polycentrism, cultural diversity, self-organisation and contextual truth is more productive and appropriate for the new epoch. Flexibility and fluidity have replaced rigidity and conformance, dynamics have replaced statics. The effort to determine the eternal unchangeables is superseded by the endeavour to capture dynamic balances and emergent phenomena.

In the Information-communication era there is a development toward a human-centrism with a potential for a new Renaissance, in which science and the humanities, arts and engineering can reach a new synthesis, through modern computing and communication tools used in global virtual societies (Dodig-Crnkovic 2003). This meeting of cultures is largely occurring in cyber space, making issues of cyber ethics increasingly important.

The Question of Values and Ethics for *E-Polis*

A view of the human, not only as a component of an automated process but as an end in itself, leads inevitably to the question of choices, values and ethics. We are not only given the world we inhabit as a fact, we are inexorably changing it.

Typical of the information-communication era is the formation of global web societies - planetary e-villages. Networking (Gill 1997, 2002) at the global level exists in the symbiotic relationship with local resources. Gill argues that a rethinking of the development idea in the contemporary globally-networked civilization is necessary. In the information society, a shift from the techno-centric to a human-centred framework is necessary in consideration of the diversity and the complexity of cross-cultural collaboration. Social cohesion in this context results from the ability to participate in the networked society through mutual interaction, exchange of knowledge and sharing of values. The relevance of associative networks for a sustainable information and communication society is discussed by Thill (1994), while Wagner, Cheung, Lee, and Ip (2003) address the related problem of enhancing e-government in developing countries via virtual communities' knowledge-management.

We are witnessing the emergence of an *e-polis* which is finding its specific ways of expression of the concept of the social good. "Policy vacuums" (Moor 1985) of a new kind of socio-technological system are being investigated, and new policies and strategies formed.

Why Privacy Matters

Before the advent of ICT, information was often spread by direct verbal communication. Today we frequently use computers to communicate and information travels far and fast, to an unlimited number of recipients, virtually effortlessly. This leads to new types of ethical problems including intrusion upon privacy. Privacy protects two kinds of basic rights:

- priority in defining ones own *identity*
  As a special case *the freedom of anonymity* can be mentioned. (In certain situations we are ready to lend our personal data for statistical investigations, for research purposes and similar, under the condition that anonymity is guaranteed.)
- the right to private *space* (generalized to mean not only physical space but also disk space or special artefacts that are exclusively connected to a certain individual, such as a private diary or private letters)

Privacy of ones' home is a classic example of a private space. It is also instructive because it shows the nature of a private space as a social construction. You are normally allowed to choose whom you wish to invite to your home. Under certain special circumstances it is however possible for police, for example, to enter your home without your consent, this being strictly regulated by law.

The following is from Article 8; Right to respect for private and family life of the British Human Rights Act (1998)

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Historically, as a result of experiences within different cultures a system of practices and customs has developed that define what is to be considered private and what is public.

According to Charles Fried (Rosen 2000), true knowledge of individuals is only achievable by persons closely related to them. Individuals have the right to choose the degree of intimacy in their relationships with other people. For a close relationship to develop there is a need of privacy and this privacy excludes the surroundings which have the role of "the others". The characteristics by which the individual is to be defined must however be decided by him/her. This is enabled through his/her rights to privacy in the sense of the control of ones' own personal information. Often when personal information is taken out of its context, there can be a risk of misinterpretation and misjudgement of a person.

An issue which might arise in policy-making is that privacy is seen differently in different parts of the world (Mizutani, Dorsey, Moor 2004). For example, there is a different attitude to privacy in Japan because of its specific cultural, linguistic and historical development. The view of privacy of a Japanese individual differs from that of an individual in the US. There is nevertheless a basic and a common understanding of privacy in any developed culture, which is called *the minimal conception of privacy*. But the culturally developed privacy in individual countries, which is called the rich conception of privacy, is what mainly differentiates the Western world and Japan in this respect. Remembering this, it is obviously difficult to establish global policies, because of the need to decide which view of privacy should be adopted. The Internet is a global technology and each part of the world has its own laws and rights to privacy.

Phenomenology of Cyber Privacy: Many (Inter)Faces of Self

"Virtual communities are a flourishing result of the free exercise of the constructionist drive. In them, users reveal personal facts, "flame", and switch personae by endlessly constructing, deconstructing and reconstructing alternative selves. They collaborate with and participate in a common social project. In general, they behave quite differently from the way they would behave in person. (..) The web empowers new categories of users with the possibility of constructing a new self and an *e-polis*." (Floridi and Sanders 2003).

Social Fraud?

Let us not forget that the social value of privacy can be questioned (Rosen, 2000). It is sometimes argued that there is a risk that the abuse of privacy rights can encourage people to conceal true information about themselves in order to gain social or economic advantages. Another opinion is that having a private life, in addition to a public life, is a social fraud which can lead to deception and hypocrisy. The counter-argument is that every society relies on *trust*. If anybody is entitled to define the characteristics of an individual, it must primarily be the individual himself/herself. By default we normally *trust* a person before we have a strong reason not to do so.

With respect to the difference between the public and the private life of a person leading to a social fraud, some see it as the wearing of different "masks" depending on the current situation in which the person is (Rosen, 2000). People wear different types of "masks" in public and in private. An influential executive who plays two different roles, depending on whether he/she is at the office with his/her colleagues or at home playing with his/her children is but one example. In general, people play different roles on different occasions and the "masks" they wear are only an expression of the different sorts of relations they have with different people.

Just How Many of You is There??

"There are many Sherry Turkles. There is the "French Sherry," who studied post-structuralism in Paris in the 1960s. There is Turkle the social scientist, trained in anthropology, personality psychology, and sociology. There is Dr. Turkle, the clinical psychologist. There is Sherry Turkle the writer of books - Psychoanalytic Politics (Basic Books, 1978) and The Second Self: Computers and the Human Spirit (Simon & Schuster, 1984). There is Sherry the professor, who has mentored MIT students for nearly 20 years. And there is the cyberspace explorer, the woman who might log on as a man, or as another woman, or as, simply, ST." (Turkle 1996).

Today's ICT-mediated experiences make the picture increasingly complex. Windows allow us to be in several contexts at the same time - in a spread sheet, in a word-processing program, in a chat room, in e-mail (ibid). Virtual spaces that many computer users could share and collaborate within, called MUDs (Multi-User Dungeons) are a new kind of social virtual reality. Obviously each user is represented by

a virtual persona created/invented for the purposes of the game. Chat personae are less obviously fictive, but they are not at all expected to correspond to real life persons. This is commonly experienced in chat rooms, and the identity problem and correspondence with the real world is settled differently from case to case according to a mutual agreement. Problems arise in situations in which reality and fiction are mixed and it becomes difficult to distinguish between the two.

Noli turbare circulos meos![1]

"Studies of cooperative work in real-world environments have highlighted the important role of physical space as a resource for negotiating social interaction, promoting peripheral awareness, and sharing artifacts [2]. The shared virtual spaces provided by CVEs (Collaborative Virtual Environments) may establish an equivalent resource for telecommunication." (Benford, Greenhalgh, Rodden, Pycock 2001).

Early studies of social interaction in CVEs stressed the interdependence between virtual and physical space. (ibid) We see the parallels between the symbolic space handling in VR and the privacy expressed as ones right to private space.

On a symbolic level, this problem can be studied in the CVEs which are virtual worlds shared by users across a computer network. Participants are represented by graphical objects called avatars that express their identity, presence, location, and activities. Avatars interact with the world and communicate via different media (audio, video, graphical gestures, and text).

Even if all the participants in CVEs are well aware of the fact that they are involved in a virtual social interplay, the CVE nevertheless presents definite reflections of their real selves. The question might be asked: Where does semblance of life stop and reality start?

"What distinguishes genuine from spurious worlds? What are worlds made of? How are they made? What role do symbols play in the making? (…) If I ask about the world, you can offer to tell me how it is under one or more frames of reference; but if I insist that you tell me how it is apart from all frames, what can you say? We are confined to ways of describing whatever is described. Our universe, so to speak, consists of these ways rather than of a world or of worlds." (Goodman 1978).

These questions, central to philosophy, are also keys to the moral understanding of the online world. Powers (2004) discusses some ethically relevant aspects of virtual, online communities by reference to more basic philosophical concepts in theories of moral realism, speech acts, and social practices. His conclusion is that in spite of the fact that "sticks and stones can break your bones, but the snerts of virtual reality can rarely hurt you… unless you let them." – virtual communities are able to *engage in real wrongs*. As any other human communities they have a capability of expressing both positive and negative intentions and feelings. With the development of ever more sophisticated techniques the expressive power of virtual reality (VR) is con-

[1] Don't upset my calculations! - Archimedes (Supposedly said in deep thoughts over geometrical shapes drawn in the sand at the moment a Roman legionary broke into his house and slew him, during the fall of Syracuse.)

stantly increasing which also leads to its more effective representation of whatever sort of relations the participants might be involved in.

Now if we agree that the real wrongs of virtual worlds can really hurt us, the question is what to do about it. What sorts of wrongs can they be? How can they be prevented?

Brey (1999) addresses ethical aspects of the design and use of VR systems, focusing on the behavioral options made available in such systems and the manner in which reality is represented or simulated in them. The representational aspects of VR applications are defined as features that articulate the way in which objects are depicted or simulated, while behavioral aspects refer to the actions or behaviors implemented in VR environments. Misrepresentation and biased representation in VR systems is one of the ethical concerns of VR especially where the virtual world and the everyday physical world are closely intertwined in a relationship.

Privacy as Architecture of Relationships

Human associations are characterized by their layered architecture which can be viewed through the degrees of privacy. The basic distinction is the one between the private (shared with a few others) and the common (shared with wider groups), (DeCew 2002). According to Mason, privacy can be studied through the relationships of four social groups:

- The first group consists of an individual, I, who has the right to privacy, both to physical privacy and to the protection of personal information.
- The second group consists of all people with whom individual I shares his/her information or private space in return for relationships or services. Individuals should acquire information about the second group before beginning a relationship with it. They must be aware of what sort of information they must provide, and how this information will be used subsequently. This type of relationship is called a negotiated relationship.
- The third group does not directly receive the information shared between I and the second group. This group has access to the information about I as a result of their professional role. The information however should not be used, since the third group is involved in activities which are irrelevant to I, who is not even aware of the fact that they might have access to such information.
- The fourth group consists of the rest of society, the public, who are not in any direct contact with I's private space or information. Tabloid newspapers profit greatly by selling private pictures of and gossip about celebrities to the public.

Each of these four social groups has its own rights and duties towards the other groups (Mason). During the interaction between groups, individuals invoke different levels of privacy. The advantages of close relationships are compared with the risks of the release of information and its inappropriate use, resulting in loss of personal space or harm to ones identity.

As mentioned before, there are differences between cultures with respect to attitudes towards privacy. That which constitutes the right to privacy is a social construction. The convention in Japan, for example, says that even if a third group were to

gain information about the first group, in a certain situation where the information was not supposed to be available, the third group should act as if the information was unknown to them (Mizutani, Dorsey, Moor 2004). An example is the network administrator who has access to private information about the students, but (s)he is supposed to act as if (s)he did not have such access.

When the rights and duties of these four groups have been settled, a technical problem raises - how to design and implement a system, which makes the information available to the groups who are entitled to the specific information at a specific time.

State of the Art: Disclosive Ethics

"While the scholarly debate continues as we define the field, it seems not unreasonable to suggest that such a task is best handled by those equipped to understand both the capabilities and limitations of the technology, on one hand, and to wield the tools of philosophical and ethical reasoning as developed over the millennia, on the other." (Vance, Information Systems Ethics page)

The classic foundational problems of computer ethics are discussed by Bynum (2000); Floridi and Sanders (2002); Floridi (1999) and Johnson (2003, 1997). Tavani (2002) gives an overview of the uniqueness debate.

For computer ethics with its specific contemporary ethical questions, Floridi and Sanders (2003) advocate the method of *ethical constructionism*. They see a parallel in the fact that there is a need for ethical policies which define the consumer's right to privacy when products and services are developed. It cannot be up to each individual to set up ethical rules for a globalized world of computer ethics. Therefore Floridi and Sanders mean that virtue ethics is not an appropriate base for computer ethics. Computer ethics is a global problem and should not be solved in a case-by-case fashion. The constructionist approach to computer ethics is, according to Floridi and Sanders better, because it does not concentrate only on the dilemmas within computer ethics faced by an individual but addresses instead, global computer ethical problems. Problems involved in, for example, the sharing and revealing of information about oneself do not only imply denial of access to the individual's information; they include more fundamental questions including the cultural and social context which must be considered when formulating policies.

Moor (1985) proposed that the central aim of computer ethics is to formulate policies to guide individual and collective action in the use of computer technology. Brey (2000) claims that not just the uses of computer technology, but also other practices that involve computing technology, such as its development and management, require the formulation of policy guidelines:

The changing resources and practices that emerge with new computer technologies yield new values, as well as requiring the reconsideration of old. There may also be new moral dilemmas because of conflicting principles that unexpectedly clash when brought together in a new context. However, according to Brey applying moral theory is only part of the computer ethicist's agenda. Privacy, for example, is now recognized as requiring more attention than it has previously received in ethics. This is due to reconceptualizations of the private and public spheres brought about by the use of

computer technology, which has resulted in inadequacies in existing moral theory about privacy. It is therefore pertinent for contemporary computer ethicists to contribute to the development of moral theory about privacy. In general, it is part of the task of computer ethics to further develop and modify existing moral theory when existing theory is insufficient or inadequate in the light of new demands generated by new practices involving ICT (Brey 2000).

For Moor, computer ethics is primarily about solving moral problems that arise because there is a policy vacuum about how computer technology should be used. In such a case, the work that is to be done is the conceptual clarification and description of the practice that generates the moral problem. Brey claims that a large part of work in computer ethics is about revealing the moral significance of practices that seem to be morally neutral. ICT has implicit moral properties that remain unnoticed because the technology and its relation to the context of its use are too complex or are not well known.

Disclosive computer ethics (Brey 2000) is a multi-level interdisciplinary approach concerned with the moral deciphering of embedded values and norms in computer systems, applications and practices. It aims to make computer technology and its uses transparent, revealing its morally relevant features. Research is performed on three levels:

- the disclosure level, at which, ideally, philosophers, computer scientists and social scientists collaborate to disclose embedded normativity in computer systems and practices,
- the theoretical level, at which philosophers develop and modify moral theory, and
- the application level, at which conclusions are drawn from research performed at the previous two levels, and at which normative evaluations of computer systems and practices takes place (Brey 2000).

The first step of the *intentional design for democracy* is the explication of the embedded moral significance of ITC where the disclosive method can be applied. The next step is to develop a technology according to human-centric principles.

Togetherness and Respect – Legitimacy by Design

"The electronic networking of physical space promises wide-ranging advances in science, medicine, delivery of services, environmental monitoring and remediation, industrial production, and monitoring of people and machines. It can also lead to new forms of social interaction, as suggested by the popularity of instant messaging (...). However, without appropriate architecture and regulatory controls it can also subvert democratic values. Information technology is not in fact neutral in its values; we must be intentional about design for democracy." (Pottie 2004).

Legitimacy is a social concept, of "socially beneficial fairness", developed during human history. It concerns social problems such as the prisoner's dilemma and the tragedy of the commons, where individuals profit but society doesn't. Social interactions without legitimacy lead society into an unstable state because of the lack of synergistic gains. Traditional mechanisms that support legitimacy, such as the law

and customs are struggling in cyberspace with its flexible, dynamic character (Whitworth and de Moor 2003).

Legitimacy analysis can translate legitimacy concepts, such as freedom, privacy and ownership of intellectual property into specific system design demands. On the other hand it can interpret program logic into statements of ownership that can be understood and discussed by a social community. Legitimate interaction, with its cornerstone of accountability, seems a key to the future of the global information society we are creating.

Whitworth and de Moor (2003) claim that legitimate interaction increases social well-being, and they analyze the ways in which societies traditionally establish legitimacy, and how the development of socio-technical systems changes previously established patterns of behaviour.

This means that democratic principles must be built into the design of socio-technical systems such as e-mail, CVE's, chats and bulletin boards. As the first step towards that goal, the legitimacy analysis of a technological artefact (software/hardware) is suggested. Legitimacy analysis can be seen as a specific branch of disclosive ethics, specialized for privacy issues.

One of the fundamental questions related to the expansion of community networks is the definition of private space vs. communal space. Spam and similar unwanted communication indicates the failure of the techno-social system which until now has not developed adequate mechanisms to prevent such privacy invasion.

As a remedy, the following three social communication "rights" are proposed:

- the right to block personal data access,
- the right to not interact, and
- the right to return e-mail to its sender.

How these requirements could be implemented is discussed by Whitworth and de Moor (2003).

Intentional Design for Democracy - Implementing Ethical Aspects in ICT

It is difficult to maintain privacy when communicating through present-day computer networks, continually divulging information about oneself. Many companies endeavour to obtain information about the potential consumer's behaviour by, for example, using cookies. [A cookie is information about a user that is stored by the server on the user's hard disk. Typically, a cookie records user's preferences when using a particular site. Web users must nominally agree to cookies being saved for them, but it commonly happens without their knowledge.]

Another method of tracing users is radio-frequency identification (RFID) of products (Pottie 2004). Identifier tags are incorporated in products and return information about the purchaser to the manufacturer. This can be an intrusion upon the consumer's right to privacy because, as a rule, the purchaser is not informed of the presence of the tag (ibid). When developing products and services today there is a need to simultaneously define the rights of the consumer. Each company should take responsibility for setting up policies concerning the ethics of their relations with consumers.

An example of the realization of *intentional design for democracy* is in the work in progress within the CyLab group at Carnegie Mellon. This includes both technical and ethics research into the development of protocols and policies that effectively balance privacy rights with Internet security. Interesting projects presented at CyLabs's web site include the following:

- *Provably Secure Steganography***.** Steganography is the process of sending a secret message in such a way that an eavesdropper is unaware that a message is being sent. In order to achieve this, messages are embedded in apparently innocent communications such as emails or photographs.
- *Secure People Location Service.* A system based on digital certificates and a public key infrastructure, which provides persons and services with information about the location of the user but gives the user fine-grain access-control over who is to be informed of his/her location. It uses a variety of mechanisms to locate people (such as calendar information, badges, wireless location, etc.), and gives users control over when information can be released and the granularity of the information. Users can also delegate access control decisions.
- *Levels of Anonymity and Traceability.* The current technical ability to track and trace Internet-based attacks is primitive. Sophisticated attacks can be almost impossible to trace to their true source using present practices. The anonymity enjoyed by today's cyber-attackers is a threat to the global information society. The aim of the ICT design must be to balance privacy and security.

Conclusion

"Growing research interest in societal issues such as work and organisational cultures, creativity and innovation, cooperation and participation, and culture and communication among AI and information technology communities shows a sign of hope for future human centred perspectives of IT research and applications. However, we must always be vigilant about the seductive nature of technical solutions of human problems and the narrowness of culture of 'short termism'." (Gill 2003).

Post-industrial society with a dominating IC technology is becoming less concerned with calculation (the primary application field of computer), and increasingly engaged in communication, less involved with machinery and more with humans. The orientation toward human-centred computing will certainly become even more apparent in the future. ICT supports and promotes the formation of new global virtual communities that are new socio-technological phenomena typical of our time. For a modern civilization of global *e-polis* the optimal functioning of virtual communities is vital.

What are the basic principles behind successful virtual community environments? According to Whitworth there are two such principles:

- Virtual community systems must match the processes of human-human interaction.
- The rights and the ownership must be clearly defined (This can actually be included under the first principle for well defined human interactions within social organizations).

ICT has the technical possibility of embedding those principles that also include privacy protection via standards, open source code, government regulation etc. (Pottie, 2004), (Tavani, Moor 2000).

Communication in contemporary cyberspace is much more then the "real-world" communication based on the identity constructed by a person involved (Floridi, Sanders 2003). This extensive freedom of identity choice has its historical reasons but it may be changed in the future (Hinde 2001, 2002). ICT design must give a balance between privacy and security in order to match the ways of traditional human-human interactions. In any computer-mediated communication, trust ultimately depends not on personal identification code number/ social security number or IP addresses but *on relationships between people* with their different roles within social groups. Trust and privacy trade-offs are normal constituents of human social, political, and economic interactions, and they consequently must be incorporated in the ICT sphere developed on the principles of human-centrism.

References

Benford S, Greenhalgh C, Rodden T, Pycock J (2001) Collaborative Virtual Environments, Commun. ACM, 44(7), 79-85

Brey P (1999) The Ethics of Representation and Action in Virtual Reality, Ethics and Information Technology 1/1, 5-14

Brey P (2000) Method in Computer Ethics: Towards a Multi-Level Interdisciplinary Approach, Ethics and Information Technology 2:3, 1-5

Bynum TW (2000) Ethics and the Information Revolution, In: G. Collste. Ethics in the Age of Information Technology. Linkoeping, Sweden: Center for Applied Ethics Linkoeping Universitet, 32-55.

Cooley MJ (1999) Invited talk at International Conference: Enterprise Cultures and Innovation in the Information Society, University of Brighton

Dodig-Crnkovic G (2003) Shifting the Paradigm of the Philosophy of Science: the Philosophy of Information and a New Renaissance, Minds and Machines: Special Issue on the Philosophy of Information, Volume 13, Issue 4

DeCew J (2002) Privacy, The Stanford Encyclopedia of Philosophy Edward N. Zalta (ed.), (http://plato.stanford.edu/archives/sum2002/entries/privacy)

Floridi L (1999) Information Ethics: On the Philosophical Foundations of Computer Ethics," Ethics and Information Technology, Vol. 1, No. 1, pp. 37-56.

Floridi L, Sanders J (2002) Mapping the Foundationalist Debate in Computer Science, a revised version of Computer Ethics: Mapping the Foundationalist Debate, Ethics and Information Technology 4.1, 1-9

Floridi L, Sanders J (2003) Internet Ethics: the Constructionist Values of Homo Poieticus. In: The Impact of the Internet on Our Moral Lives, Robert Cavalier ed.

Gill, KS (1997) Knowledge networking and social cohesion in the Information Society, a study for the European Commission

Gill KS (2002) Knowledge Networking in Cross-Cultural Settings, AI & Soc 16: 252-277

Gill KS (2003) Future with AI & Society (http://www.it.bton.ac.uk/research/seake/ai_soc6_3.html)

Goodman N (1978) Ways of Worldmaking, Indianapolis: Hackett Publishing
Human Rights Act 1998 http://www.hmso.gov.uk/acts/acts1998/80042--d.htm
Hinde S (2001) 2001: A Privacy Odyssey. Computers and Security, Vol. 20
Hinde S (2002) 2001: A Privacy Odyssey Revisited. Computers and Security, Vol. 21
Johnson DG (1997) Ethics Online. Association for Computing Machinery. Communications of the ACM.
Johnson DG (2003) Computer Ethics. The Blackwell Guide to the Philosophy of Computing and Information. Edited by Luciano Floridi. Blackwell Publishing
Research Projects at Carnegie Mellon CyLab (http://www.cylab.cmu.edu/default.aspx?id=10)
Mason RO, A tapestry of Privacy, A Meta-Discussion. (http://cyberethics.cbi.msstate.edu/mason2/)
Mizutani M, Dorsey J, Moor JH (2004) The internet and Japanese conception of privacy. Ethics and Information Technology
Moor JH (1985) What is computer ethics? Metaphilosophy 16/4. (http://www.ccsr.cse.dmu.ac.uk/staff/Srog/teaching/moor.htm)
Pottie GJ (2004) Privacy in the Global Village, Communications of the ACM, 47(2): 2-23
Rosen J (2000) Why Privacy Matters, Wilson Quarterly. Vol 24, Issue 4
Powers TM (2004) Real wrongs in virtual communities, Ethics and Information Technology, Volume 5, Issue 4, 191-198
Sixth Programme (FP6) of the European Union, Citizens and governance in a knowledge-based society theme. (http://www.cordis.lu/fp6/citizens.htm)
Tavani H. (2002) The uniqueness debate in computer ethics: What exactly is at issue, and why does it matter?, Ethics and Information Technology 4: 37–54, and references therein
Tavani HT, Moor JH (2000) Privacy Protection, Control of Information, and Privacy-Enhancing Technologies. Proceedings of the Conference on Computer Ethics-Philosophical Enquiry
Thill, G (1994), The relevance of associative networks for a sustainable information and communication society, AI and Society, 6.1: 70-77
Turkle, S. (1996). Who am we? Wired, 4(1), 148-152, 194-199
Vance, D. The Place of Cyberethics, Information Systems Ethics, (http://cyberethics.cbi.msstate.edu/)
Wagner, C, Cheung K, Lee F, Ip R (2003) Enhancing e-government in developing countries: managing knowledge through virtual communities. The Electronic Journal on Information Systems in Developing Countries, 14, 4, 1-20
Whitworth B, de Moor, A (2003) Legitimate by design: Towards trusted virtual community environments. Behaviour and Information Technology 22:1, p31-51.