Privacy and Protection of Personal Integrity in the Working Place

Dodig-Crnkovic G

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

Abstract

Privacy and surveillance is a topic with growing importance for working places. Today's rapid technical development has a considerable impact on privacy. The aim of this paper is an analysis of the relation between privacy and workplace surveillance. The existing techniques, laws and ethical theories and practices are considered.

The workplace is an official place par excellence. With modern technique it is easy to identify and keep under surveillance individuals at the workplace where everything from security-cameras to programs for monitoring of computer usage may bring about nearly a total control of the employees and their work effort.

How much privacy can we expect at our workplaces? Can electronic methods of monitoring and surveillance be ethically justified? A critical analysis of the idea of privacy protection versus surveillance or monitoring of employees is presented.

One central aspect of the problem is the trend toward the disappearance of boundaries between private and professional life. Users today may work at their laptop computers at any place. People send their business e-mails from their homes, even while travelling or on vacations. How can a strict division be made between private and official information in a future world pervaded with ubiquitous computers?

The important fact is that not everybody is aware of the existence of surveillance, and even fewer people are familiar with privacy-protection methods. That is something which demands knowledge as well as engagement. The privacy right of the working force is grounded in the fundamental human right of privacy recognized in all major international agreements regarding human rights such as Article 12 of the Universal Declaration of Human Rights (United Nations, 1948).

The conclusion is that trust must be established globally in the use of ICT (information and communication technology), so that both users (cultural aspect) and the technology will be trustworthy. That is a long-term project which already has started.

Keywords: Privacy, Cyberethics, Ethics of Trust, Legitimate by design, Disclosive ethics, Intentional design for democracy.

INTRODUCTION

A characteristic of private is that it is not official. Nevertheless, we expect a certain degree of privacy even in the most official situations. Privacy is a fundamental human right recognized in all major international agreements regarding human rights such as Article 12 of the Universal Declaration of Human Rights (United Nations, 1948). But just how much privacy can we expect at the workplace,

where in some cases we may be subject to surveillance? Can electronic methods of monitoring and surveillance be ethically justified? We present a critical analysis of the idea of privacy protection versus surveillance or monitoring of employees, based on the data from different cultures with a wide range of practices.

One important aspect of the problem of privacy at the workplace is the trend toward the disappearance of boundaries between private and professional life, when working hours are no longer fixed, when people work at their laptop computers at all places imaginable, following the trend toward the ubiquitous use of the computer. Ubiquitous computing is the third wave, now beginning, in the use of the computer. The first computers were mainframes, the second era, in which we are now, is the personal computing era. Next comes ubiquitous computing, with the computing merged into the background of our lives.

Already, many people send their business-related e-mails from their homes, from airports, while traveling or even on vacations. How can a strict division be created between private and official information in a future world pervaded with the use of computers for both official and private purposes?

MODERN ELECTRONIC MONITORING AND SURVEILLANCE

The four basic **S**'s of computing technology (**S**earching, **S**orting, **S**torage and **S**imulation) make computers unprecedented tools of control. The ease with which data stored in a computer can be manipulated, as if it were greased (Moor, 2004) makes the use of monitoring, surveillance, and spyware methods extremely easy from the technical point of view. The consequences of the use of modern computation and communication tools in this connection are interesting both from the viewpoint of the individual employee (citizen) and from that of society.

Present-day surveillance tools include closed circuit television (CCTV), night vision systems, miniature transmitters, smart cards, electronic beepers and sensors, telephone taps, recorders, pen registers, computer usage monitoring, electronic mail monitoring, cellular radio interception, satellite interception, radio frequency identification (RFID), etc.

There are indications that the use of monitoring at workplaces has increased and is likely to continue to increase rapidly in coming years (Wakefield, 2004). The issues of concern leading to such surveillance are business information protection, the monitoring of productivity, security, legal compliance and liability, inter alia by means of e-mail-, spam-, pornography- and similar filters.

There is in fact, already legislation in various countries permitting the monitoring of employees by their employers and one-third of the work force in the US working on-line is under surveillance [Hinde (2002)]. VIDEO is a report summarizing an investigation of video surveillance practices in a number of countries (certain European countries, USA, Australia and Canada) and their effects on privacy. Here are some of its conclusions.

"The evidence presented to the Inquiry suggests that video surveillance has the potential to have a far greater impact on the privacy of employees than is evident presently."

"Covert surveillance involves an extremely serious breach of employee privacy. Evidence presented to the Inquiry indicates that there is an urgent need for measures to address the use of covert video surveillance in workplaces. Without any legislative protection, employees have no protection against secret and ongoing surveillance in the workplace. These measures are needed to address the inconsistency in current legislation, which prohibits the covert use of listening devices (refer Paragraph 5.1.2.2), but gives no protection from covert video surveillance. This inconsistency is best explained as the result of regulation being outpaced by technology."

Further, the VIDEO report states that:

"Although regulation on video surveillance in workplaces in industrialized nations is still taking shape, many countries have already imposed limitations on its use. It reflects a belief that video surveillance in the workplace is a threat to employees' rights to privacy, dignity and personal autonomy. The two main targets for regulation are covert surveillance and the use of surveillance for monitoring individual employee work practices. The sources of these protections have been the application of constitutional, common law or application of fundamental human rights; privacy and data protection legislation; industrial relations legislation."

Advocates of workplace monitoring claim that it nevertheless might be an acceptable method when justified by business interests (Wakefield, 2004). However, recent studies show that employees under surveillance feel depressed, tense and anxious when knowing that they are monitored (Uyen Vu, 2004), in comparison with those who are not under (or who are unaware of) surveillance (Rosen, 2000). Psychologists consider that it is obvious that an individual (who knows/suspects that he/she is) under surveillance behaves differently from another not monitored, the monitored person restricting his/her actions, aware that they are being observed by a suspicious third party. The climate of distrust is detrimental to the motivation, creativity and productivity of employees.

The report for the European Parliament, carried out by the parliament's technology assessment office, says the use of CCTV should be addressed by the MEP's Committee on Civil Liberties and Internal Affairs, because the technology facilitates mass and routine surveillance of large segments of the population. Automated face or vehicle recognition software allows CCTV images to be digitally matched to pictures in other databases, such as the photographic driver licenses now planned in Britain. The unregulated use of such a system would amount to an invasion of privacy, says the report, (MacKenzie, 1997)

WHY VALUE PRIVACY? PRIVACY AND DEMOCRACY

A brief analysis of the phenomenon of privacy protection and its importance for democracy is given in (Moor, 2004), beginning with Moor's justification of privacy as the expression of a core value of security. The question arises consequently: How should situations be addressed in which privacy and security are complementary? There are namely situations in which more privacy for some people means less security for others.

In Warren and Brandeis' argument, privacy stems from a representation of selfhood which they call "the principle of inviolate personality" and personal self possession. Charles Fried claims that human feelings such as respect, love and trust are unimaginable without privacy, meaning that intimacy and privacy are essential parts in relationships. Privacy is not merely an instrumental value to achieve further ends such as respect and trust; it is also seen as having an intrinsic value in human life.

According to Rosen (2000), privacy has political, social and personal values and costs. The political value involves the fact that there is no need to reveal one's rank or family background, to be able to interact with others in a democracy. Thanks to privacy, it is possible for citizens, who might disagree on a topic, to communicate with each other without needing to reveal the details of their identity. Privacy reaches beyond individual benefit by being a value which contributes to the broader good, becoming an essential element of democracy (Grodzinsky and Tavani, 2004). In intruding on privacy, which is closely related to freedom, surveillance can be considered to have, ultimately, a negative effect on democracy.

By its nature, computer ethics is a worldwide phenomenon and cannot be tackled exclusively on an individual and local scale, (Johnson, 2003). For computer ethics with its specific contemporary questions, Floridi and Sanders (2003) advocate the method of ethical constructionism. The constructionist approach concentrates not only on the dilemmas faced by the individual but also addresses global computer ethics problems. Issues involved in e.g. the sharing and revealing of information about oneself introduce even more fundamental questions including the cultural and social context which must be considered when formulating policies.

LEGISLATION

"Technology can go a long way toward protecting the privacy of individuals, but we also need a legal framework to ensure that technology isn't outlawed (Bernstein: http://www.eff.org/bernstein/.) We can't protect privacy through case law, and self-regulation hasn't worked."

Deborah Pierce

Privacy is a fundamental human right recognized in all major international treaties and agreements on human rights, as stated in Article 12 of the Universal Declaration of Human Rights (United Nations, 1948).

Article 12.

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Article 17 of the UN’s International Covenant on Civil and Political Rights (see ICCPR), uses essentially the same formulation as Article 12.

Nearly every country in the world recognizes privacy as a basic human right in their constitution, either explicitly or implicitly. Most recently drafted constitutions include specific rights to access and control one's personal information (Council of Europe Convention and Legislation Links). According to PRIVACY AND HUMAN RIGHTS report:

“Interest in the right of privacy increased in the 1960s and 1970s with the advent of information technology (IT). The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information. In many countries, new constitutions reflect this right. The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970 This was followed by national laws in Sweden (1973), the United States (1974), Germany (1977) and France (1978). [fn 34]

Two crucial international instruments evolved from these laws. The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data [fn 35] and the Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data [fn 36] articulate specific rules covering the handling of electronic data. The rules within these two documents form the core of the Data Protection laws of dozens of countries. These rules describe personal information as data which are afforded protection at every step from collection through to storage and dissemination. The right of people to access and amend their data is a primary component of these rules.

The expression of data protection in various declarations and laws varies only by degrees. All require that personal information must be:

- obtained fairly and lawfully;
- used only for the original specified purpose;
- adequate, relevant and not excessive to purpose;
- accurate and up to date; and
- destroyed after its purpose is completed.”

New technologies are increasingly threatening privacy. These include video surveillance cameras, identity cards and genetic databases.

There is a growing trend towards the wide-ranging privacy and data protection acts around the world. Currently over 40 countries have already adopted or are in the process of adopting such laws, among others to promote electronic commerce and to ensure compatibility with international standards developed by the European Union, the Council of Europe, and the Organization for Economic Cooperation and Development.

The worldwide development of digital government services makes questions of digital privacy increasingly important. The way classical government has been organized historically, with separate departments with their own personal data banks has inherently provided some privacy protection through practical anonymity, data matching being expensive in a distributed environment, (Hansen, Pfitzmann, 2004). The advent of IC technology has made data matching technically extremely easy.

Moreover, a huge amount of data is collected by non-governmental organizations in business and the like, making commercial Little Brother, in addition to governmental Big Brother (McCrone, 1995) a potential threat to privacy, further complicating the situation. As the remedy Hes and Borking (2000) present privacy-enhancing technologies protecting anonymity. Hansen and Pfitzmann (2004) give a terminological analysis of identity management including anonymity, unobservability and pseudonymity.

Data protection law, in spite of its central importance, cannot cover the entire digital privacy field. It focuses mostly on the larger databases and their use (Wayner, 2004) and disregards other privacy-related problems, notwithstanding the fact that many privacy-invasive technologies acquire digital records that should be subject to data protection. Examples of such potentially privacy-invasive technologies are different positioning devices, RFID and video surveillance, whose results may not be recorded, although they can still be a threat to privacy.

ETHICS OF TRUST

Trust is one of the building blocks of a civilized society. We trust train and airline time-tables and plan our journeys accordingly, we trust the pharmaceutical industry in taking their pills, believing that they will cure us and not kill us, we trust our employers and colleagues, assuming that what they promise or claim is what they, at least, believe to be true. As any other factor in human relations, trust has many different aspects in the different contexts. Wittgenstein's dictum `meaning is use' applies here as well. One can consider trust as a cognitive process or state, within the psychology of personality as a behavioral/developmental process, as a social psychology/sociology related phenomenon. In connection with cultural history and privacy, it is influenced by and influences social politics and society at large, for example, defining our responsibilities (Kainulainen, 2001).

Hinman (2002) puts it in the following way: “Trust is like the glue that holds society together -- without it, we crumble into tiny isolated pieces that collide randomly with one another. In a world without trust, individuals cannot depend on one another; as a result, individuals can only be out for themselves. Economists have shown that societies where trust is low have stunted economic growth because a robust economy demands that individuals be able to enter into cooperative economic relationships of trust with people who are strangers.”

Hinman claims that trust is one of the three universal core values found across cultures:

- caring for children;
- trust;
- prohibitions against murder.

This even holds in the most primitive artificial (computer-simulated) populations, in that case having the following effects:

- assuring the continuity of population in terms of number of individuals and ways of behavior;
- respecting the commonly accepted set of rules, which provides predictability and stable relationships;
- preventing the extinction of the population.

Trust thus has deep roots in both the needs of individual humans for security, safety, confidence and predictability and in the basic principles of social dynamics.

One field that has traditionally focused on the problem of trust is medical ethics. In Francis (1993) the section ‘Ethics of Trust vs. Ethics of Rights’ discusses autonomy, informed consent and the rights of patients. The relationship of dependence and usually significant difference in knowledge, which characterises doctor-patient communication and the position of the patient within the health-care system, have its counterpart in the relation between a common computer user and a computer professional knowing how to configure the machine or the network and communication in ways that

have significant consequences for the user. Basically, the relation between a specialist and a lay-person is that of power and subjection and must be grounded on mutual trust.
Historically, however, such unconditional trust on the part of the general public in the inherent goodness of technology has been shown to be unwarranted.
Technology is far too important to everybody to be left to the specialist alone. Agre (1994) says "The design of computer systems has not historically been organized in a democratic way. Designers and users have had little interaction, and users have had little control over the resulting systems, except perhaps through the indirect routes available to them through resistance in the workplace and the refusal to purchase relatively unusable systems for their own use. Yet over the last ten or twenty years, a growing movement, originating in Scandinavia but now increasingly influential in other industrialized countries, is attempting to reform the design of computer systems in a more democratic direction (Bjerknes, Ehn, and Kyng 1987, Schuler and Namioka 1993). This movement, sometimes known as *participatory design*, invites the participation of, and in many cases gives formal control over the design process to, the people whose work-lives the system affects."
Here one can add "Weiser's principle of Inventing Socially Dangerous Technology:

1. Build it as safe as you can, and build into it all the safeguards to personal values that you can imagine.

2. Tell the world at large that you are doing something dangerous."

Weiser, 1995

This principle aims at the establishment of a trust relationship between the specialists (inventors of dangerous technologies) and common users (people who are affected by the potentially dangerous consequences of technology).

LEGITIMACY BY DESIGN AND TRUSTWORTHY COMPUTING

"Trust is a broad concept, and making something trustworthy requires a social infrastructure as well as solid engineering. All systems fail from time to time; the legal and commercial practices within which they're embedded can compensate for the fact that no technology will ever be perfect. Hence this is not only a struggle to make software trustworthy; because computers have to some extent already lost people's trust, we will have to overcome a legacy of machines that fail, software that fails, and systems that fail. We will have to persuade people that the systems, the software, the services, the people, and the companies have all, collectively, achieved a new level of availability, dependability, and confidentiality. We will have to overcome the distrust that people now feel for computers.
The Trustworthy Computing Initiative is a label for a whole range of advances that have to be made for people to be as comfortable using devices powered by computers and software as they are today using a device that is powered by electricity. It may take us ten to fifteen years to get there, both as an industry and as a society.
This is a "sea change" not only in the way we write and deliver software, but also in the way our society views computing generally. There are immediate problems to be solved, and fundamental open research questions. There are actions that individuals and companies can and should take, but there are also problems that can only be solved collectively by consortia, research communities, nations, and the world as a whole."

Mundie, at al. (2003)

It is apparent that the problem of trust involves more than the establishment of decent privacy standards; it concerns even security, reliability and business integrity. The Trustworthy Computing Initiative is an indication of how serious the problem is and how urgent is its solution for the development of a society supported by computer technology. It is good news that business shows awareness of the social impact of the technology they produce and understanding of how basic public acceptance, confidence and trust is for the general direction of the future development of society. It gives hope that at least some important aspects of privacy problems of today will be solved within the decades to come.

The first phase of the *intentional design for democracy* is the explication of the embedded moral significance of ICT while the next is the development of the corresponding technology (Yu and Cysneiros, 2002). The existing analyses of the state of the art of privacy issues worldwide (fifty countries in http://www.gilc.org/privacy/survey) bear witness to how much work remains to be done.

"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. Traditional mechanisms that support legitimacy such as the law and customs are not yet well defined in cyberspace with its flexible, dynamic character. 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, (Dodig-Crnkovic, Horniak, 2005).

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 necessary. Legitimacy analysis can be seen as a specific branch of disclosive ethics, specialized for privacy issues. Fischer-Hübner (2001) adress the problem of IT-security and privacy, discussing the design and use of privacy enhancing security mechanisms.

What we as users have a right to expect in the near future is that the ICT follows Privacy/Fair Information Principles: "Users are given appropriate notice of how their personal information may be collected and used; they are given access to view such information and the opportunity to correct it; data is never collected or shared without the individual's consent; appropriate means are taken to ensure the security of personal information; external and internal auditing procedures ensure compliance with stated intentions." (Mundie, at al., 2003)

Whose Responsibility? Agency and Surrogate Agency

According to Kainulainen (2001), A Trust and Ubiquitous Computing, the layers of trust are as follows:

- Individual - machine
- Individual - individual
- Individual - (machine) - individual
- Individual - identifiable small groups (social aspect)
- Individual - groups/organizations (authority, higher levels of hierarchy and abstraction)
- Group - group

As a consequence, a question arises: how, in all these types of interactions, to establish the responsibility, especially when machines and software agents (e.g. intelligent software agents such as web bots - 'software robots') are involved. Johnson and Powers (2004) study the problem of the responsibility of (autonomous) agents which are used as role or "surrogate" mediators to pursue the interests of their clients. We are familiar with surrogate agents who usually act as stockbrokers, lawyers, and managers, performers and entertainers. It is an established praxis that when the behavior of a surrogate agent falls below a certain standard of diligence or authority, the client can sue the agent and the agent can be found liable for his or her behavior. This suggests that similar criteria should be developed with respect to computer agents. Questions arise about the rights and responsibilities of

computer agents, their owners and designers. These are matters that should be highlighted and regulated in the immediate future. The surrogate agents already in operation are obvious candidates for a thorough ethical analysis.

CONCLUSION

"Yes, safeguards can be built into any system, such as the checks and balances in a good accounting system. But what keeps them in place is not the technology, but people's commitment to keeping them.

We cannot expect technology alone to solve ethical dilemmas. Technology is a tool made by people to meet people's needs. Like all tools, it can be used in ways undreamed of by the inventor. Like all tools, it will change the user in unexpected and profound ways."

Weiser (*1995)*

Koehn (1998) makes the following list of characteristics that an ethic should possess. It:

- requires each of us to properly appreciate other human beings' distinctive particularity;
- acknowledges the extent to which we are thoroughly interdependent beings;
- imposes limits on the extent to which we are obligated to be open to others;
- engenders the self-suspicion necessary if our relations are to be free of manipulation, narcissism, self-righteousness and unjust resentment and
- provides for a rule of law and for political accountability.

After analyzing several kinds of ethic (an ethic of care, an ethic of broad empathy, an ethic of trust and a dialogical ethic) Kohen finds all of the above elements in a dialogical ethic. Its main feature is *interactivity and dynamic*, and it is based on the culture of trust. That is how the problem of workplace privacy can be seen. It is a part of a more general problem of privacy, and in the digital era, life in a global, networked E-village implies that the problem must be solved on a global level. Not only through legislation (even though it is very important building block), not only through technology (even thought it is essential), but through an informed ethical dialogue.

Our conclusion is that mutual trust which is one of the basic ethical principles on which human societies rely must be established in the use of ICT. This in the first place presupposes the informed consent of all the parties involved as a conditio sine qua non. Moreover, trust must also be established globally because the data contained in networked computers virtually knows no boundaries, and is easy to manipulate.

REFERENCES

Agre, E. P. (1994) Design for Democracy, http://polaris.gseis.ucla.edu/pagre/oksnoen.html

Dodig-Crnkovic, G. and Horniak, V. (2005), Good to Have Someone Watching Us from a Distance? Privacy vs. Security at the Workplace, *Ethics of New Information Technology, Proceedings of the Sixth International Conference of Computer Ethics: Philosophical Enquiry, CEPE 200, July 17-19, 2005, University of Twente, Enschede, The Netherlands ;* Brey P,Grodzinsky F and Introna L. Eds. http://cepe2005.utwente.nl/

Grodzinsky, F.S., Tavani, H.T. (2004) Verizon vs. The RIAA: Implications for Privacy and Democracy, IEEE, 0-7803-8251-x

Fischer-Hübner, S. and G. (2001). *IT-Security and Privacy: Design and Use of Privacy Enhancing Security Mechanisms*. Lecture Notes in Computer Science, Vol. 1958. Berlin Heidelberg: Springer-Verlag

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

Francis, C.M. (1993) Medical Ethics, Jaypee Brothers Medical Publishers (Pvt) Ltd) New Delhi

Hansen, M., Pfitzmann, A. (2004). *Anonymity, Unobservability, Pseudonymity, and Identity Management – A Proposal for Terminology*, v0.21. http://dud.inf.tu-dresden.de/Literatur_V1.shtml

Hes, R. and Borking, J. (Eds.) (2000) *Privacy-enhancing technologies: The path to anonymity*. Revised edition. Registratiekamer, The Hague, August 2000. http://www.cbpweb.nl/downloads_av/AV11.PDF

Hinde, S. (2002) 2001: A Privacy Odyssey Revisited. *Computers and Security*, Vol. **21**, No. 1

Hinman, L.M. (2002) A Moral Challenge: Business Ethics after Enron, The San Diego Union-Tribune. http://ethics.acusd.edu/LMH/op-ed/Enron/

Johnson, D.G. (2003) Computer Ethics. *The Blackwell Guide to the Philosophy of Computing and Information*. Luciano Floridi Ed. Blackwell Publishing

Johnson, D.G. and Powers, M.T. (2004) Computers as Surrogate Agents, ETHICOMP 2004 http://www.ccsr.cse.dmu.ac.uk/conferences/ethicomp/ethicomp2004/abstracts/96.html

Kainulainen, A. (2001) Trust and Ubiquitous Computing, http://www.cs.uta.fi/~anssi/work/cogscisempres_7.4.2001.ppt#258,1,Trust%20and%20Ubiquitous%20Computing

Koehn, D. (1998) *Rethinking Feminist Ethics: Care, Trust and Empathy*, Routledge

MacKenzie, D. (1997) Privacy police caution Big Brother. *New Scientist* vol **154** - 12, p4

McCrone, J (1995) Watching you, watching me. *New Scientist*, 36-9

Moor, J.H. (2004) Towards a Theory of Privacy in the Information Age. *Computer Ethics and Professional Responsibility*, Bynum, T.W. and Rogerson, S. Edts., Blackwell Publishing

Mundie, C., de Vries, P., Haynes, P. and Corwine M, (2003) Trustworthy Computing White Paper http://www.microsoft.com/mscorp/twc/twc_whitepaper.mspx

Pierce D., Challenges/Threats to Privacy http://www.inetdevgrp.org/20001017/index.html

Pottie, G.J. (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

Vu Uyen (2004) Employees resistant to any form of computer video monitoring, study says. *Canadian HR Report*, March 8

Wakefield, R.L. (2004) Computer Monitoring and Surveillance – Balancing Privacy with Security. The CPA Journal

Warren, S.D. and Brandeis, L.D. (1890) The Right to Privacy, *Harvard Law Review*, **1890-91**, No.5, 193-220. http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html

Weiser, M. (1995) The Technologist's Responsibilities and Social Change, *Computer-Mediated Communication Magazine*, Vol. **2**, No. 4, p. 17

Wayner, P. (2004) The Power of Candy-Coated Bits. *IEEE Security & Privacy*, Vol. 2, No. 2, March-April 2004, 69-72.

Whitworth, B. and de Moor, A. (2003) Legitimate by design: Towards trusted virtual community environments. *Behaviour and Information Technology* **22:1**, p31-51.

Yu, E. and Cysneiros, L. (2002) Designing for Privacy and Other Competing Requirements. *2nd Symposium on Requirements Engineering for Information Security (SREIS'02)*, Raleigh, North Carolina, October 16, 2002. http://www.cs.toronto.edu/pub/eric/SREIS02-Priv.pdf

Books

Hansson, S O and Palm E., *The Ethics of Workplace Privacy*, Peter Lang Bruxelles 2005

Dalenius T. and Klevmarken A., *Proceedings of a Symposium on Personal Integrity and the Need for Data in the Social Sciences*, Held at Hasselby Slott, Stockholm March 15-17, 1976 and Sponsored by the Swedish Council for Social Science Research, Swedish council for social science research

Bennett, Colin J. and Charles J. Raab, *The Governance of Privacy:Policy Instruments in Global Perspective*, Aldershot: Ashgate, 2002

Flaherty, David H., *Protecting Privacy in Surveillance Societies: the Federal Republic of Germany, Sweden, France, Canada, & the United States*, University of North Carolina Press, Chapel Hill, 1989

Legislation links

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.: 108
http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&CL=ENG

EU Directive 95/46/EC (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L 281, 23/11/1995*, pp. 31-50.
http://europa.eu.int/eur-lex/en/index.html

European Council Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data CETS No.: 108
http://conventions.coe.int/treaty/EN/WhatYouWant.asp?NT=108&CM=8&DF=

Data Protection Guide http://www.europa.eu.int/comm/internal_market/privacy/index_en.htm

GUIDES (2002). E-Business Guidelines on DPD 95/46/EC.
http://eprivacyforum.jrc.it/default/page.gx?_app.page=entity.html&_app.action=entity&_entity.object=KM------00000000000002C8&_entity.name=guidelines.pdf

von Lohmann F, Meditations on Trusted Computing http://www.nr.no/~abie/TrustPolicy.htm

ICCPR http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

OECD (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*
http://www1.oecd.org/publications/e-book/9302011E.PDF

OECD (2005) European Data Protection Supervisor
http://www.europa.eu.int/comm/internal_market/en/dataprot/inter/priv.htm

The Dutch Data Protection Authority (2001). Privacy Audit Framework under the new Dutch Data Protection Act (WBP), April 2001.
http://www.cbpweb.nl/en/download_audit/PrivacyAuditFramework.pdf

Treasury Board of Canada Secretariat (2002). Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld-PR_e.asp?printable=True

United Nations (1948). *Universal Declaration of Human Rights*, General Assembly resolution 217 A (III). http://www.un.org/Overview/rights.html

UN guidelines http://www.europa.eu.int/comm/internal_market/en/dataprot/inter/un.htm

Other resources

http://www2.austlii.edu.au/itlaw/articles/efficiency.html#Heading2 Graham Greenleaf: Stopping surveillance: Beyond 'efficiency' and the OECD

http://www.worldlii.org/int/special/privacy/ Australian Privacy Law Project

http://www.worldlii.org/catalog/273.html WorldLII Catalog >>Privacy

http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html Introduction to Dataveillance and Information Privacy, and Definitions of Terms Roger Clarke

http://www.arts.ed.ac.uk/asianstudies/privacyproject/bibliographyNK.htm Materials in Western languages on privacy issues

All links retrieved at December 19, 2005