GOOD TO HAVE SOMEONE WATCHING US FROM A DISTANCE?

Privacy vs. Security at the Workplace
CONTENTS

- INTRODUCTION
- PRIVACY DEFINITIONS
- MONITORING AND SURVEILLANCE
- SURVEILLANCE TOOLS
- LEGISLATION
- WHOSE RESPONSIBILITY? AGENCY AND SURROGATE AGENCY
- THE UNIVERSAL CORE VALUES FOUND ACROSS CULTURES
- TRUST AND WORKPLACE PRIVACY
- INVENTING SOCIALEY DANGEROUS TECHNOLOGY
- ETHICS OF TRUST
- LEGITIMACY BY DESIGN AND TRUSTWORTHY COMPUTING
- CONCLUSIONS
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).
INTRODUCTION

- Privacy protection vs. surveillance of employees
- Disappearance of boundaries between private and professional life:
  - ubiquitous computing and
  - ambiental intelligence
MONITORING AND SURVEILLANCE

- Searching,
- Sorting,
- Storage
- Simulation

- the four basic S’s of computing technology that makes it unprecedented tools for monitoring and surveillance
SURVEILLANCE TOOLS

- Closed Circuit Television (CCTV)
- Night vision system
- Smart cards
- Telephone taps
- Computer usage (E-mail monitoring, Internet monitoring and filtering, instant message monitoring, keystroke logging)
- Cellular radio/Satellite interception
- Radio Frequency Identification (RFID)
- Location monitoring
- ...
SURVEILLANCE TOOLS

- VIDEO
  - Greater impact on the privacy of employees than is evident presently
  - Serious breach of employee privacy
  - Many countries have imposed limitations on workplace surveillance
  - Justified by business interests (Wakefield)
“The predominant view among the experts was that since nowadays almost all economic information is exchanged through electronic means (telephone, fax, e-mail), and, in addition, all digital telecommunication devices and switches have enhanced wiretapping capabilities, for these reasons they suggested that we must focus on the protection of the data when transmitted (using encryption products), on the use of government-approved encryption products and on the adoption of common standards concerning encryption and key-recovery products.”
The position could be summed up in the statement that 'since it is difficult to prove that economic information has been captured by ECHELON system and passed on by the NSA, we have to consider privacy protection in a global international networked society'.

(European Parliament, Scientific And Technological Options Assessment; Development Of Surveillance Technology And Risk Of Abuse Of Economic Information)
- Face
- Fingerprint / Palm Print
- Hand and Finger Geometry
- Handwriting
- Iris
- Voice/Speaker
- Retinal
- Multimodal
The Universal Declaration of Human Rights – 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.”

UN’s International Covenant on Civil and Political Rights (ICCPR)
The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data

The Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data
The layers of trust, Kainulainen (2001):

- 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

Johnson and Powers (2004) study the problem of the responsibility of (autonomous) agents which are used as role or "surrogate" mediators.
In intruding on privacy, which is closely related to freedom and autonomy, surveillance can be considered to have, ultimately, a negative effect on democracy.
PRIVATE AND HUMAN RIGHTS Report

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
Caring for children;

Trust;

Prohibitions against murder.

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.

(Hinman)
TRUST AND WORKPLACE PRIVACY

- Parallels between Computer Ethics and Medical Ethics: Francis (1993) in the section ‘Ethics of Trust vs. Ethics of Rights’ discusses autonomy, informed consent and the rights of patients.

- Basically, the relation between a specialist and a lay-person is that of power and subjection and must be grounded on mutual trust.
Historically an unconditional trust on the part of the general public in the inherent goodness of technology has been shown to be *unwarranted*. 
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).

Agre (1994)
“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
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
CODES OF ETHICS
(Primarily Targeting Designers)

- ACM (Association for Computing Machinery)
- BSC (British Computer Society)
- IEEE (Institute of Electrical and Electronics Engineers)
- DataForum
- CF (Civilingenjörsförbundet)
Whether or not privacy is protected by law or contract, fostering a workplace culture where privacy is valued and respected contributes to healthy human relations, and makes good business sense.
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.
LAYERS OF TRUST

• Trust in the intent of designers
• Trust in the quality of workmanship
• Trust in the users
“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.”

Hinman (2002)
CONCLUSIONS

TRUST must be established in the use of ICT, where both users and the technology will be trustworthy.

This in the first place presupposes the INFORMED CONSENT of all the parties involved.

This trust must be established GLOBALLY because the data contained in networked computers virtually knows no boundaries.
Gordana Dodig-Crnkovic, Virginia Horniak
*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 2005
July 17-19, 2005, University of Twente, Enschede, The Netherlands; Brey P, Grodzinsky F and Introna L. Eds.