

# Wireless Environments & Privacy

Patricia S. Taylor  
Eastern Illinois University

&

Robert E. McGrath  
NCSA, University of Illinois

EDRA

Vancouver, BC -- May 2005

# Introduction

- Views from a Social Scientist and a Computer Engineer
- Privacy
- Wireless devices & environments
- Design issues

# Privacy – Behavioral View

Control over access

Cultural & individual values vary

Mechanisms of control

Verbal behavior

- œ Lower voice

- œ Let's talk

Environmental

- œ Open door

Nonverbal behavior

- œ Body language

- œ Eye contact

Cultural

- œ Dropping by

# New Facets of Privacy: Control over Information

- Empowerment
  - Informational privacy
- Utility
  - Protection against intrusion
- Dignity
  - Equilibrium of information between people or person and institution
- Regulating agent
  - Checks and balances on decision-makers

# Self-Presentation

- Face-to-face – verbal & nonverbal cues
  - Who am I? Who am I interacting with?
- How might self-presentation change when individual notices surveillance?
  - If you believe you are pretty much anonymous?
    - (videocam at supermarket)
  - If you believe you can be identified?
    - (videocam at work)

# Wireless Devices

- Computers, phones, cameras, locational devices (GPS, RFID)
- Sensors beyond human capacity
- Smart-Its – adding sensor capability to objects in the environment

# Benefits of Wireless Devices

- Education
  - Link field data to classroom
- Health care
  - Monitor chronic patients from their homes
  - Welfare and safety of elderly & disabled
- Human interaction and communication
  - Both remote and in person

# Wireless Environments

- Passive
  - Access to networks
  - Monitor of local activity/environment status
- Active
  - Promote
    - Human-information interaction
    - Human-human cooperation
  - Control environment (lights, heat, access)

# Scale of Environments

- City
- Neighborhood
- Building
- Floor/Room
  
- Varying needs for access, privacy, security
- Varying opportunities to promote positive human interactions

# Legal Issues

1. Openness and transparency
2. Individual participation
3. Collection limitation
4. Data quality
5. Use limitation
6. Reasonable security
7. Accountability

# Current Issues – Tech & Privacy

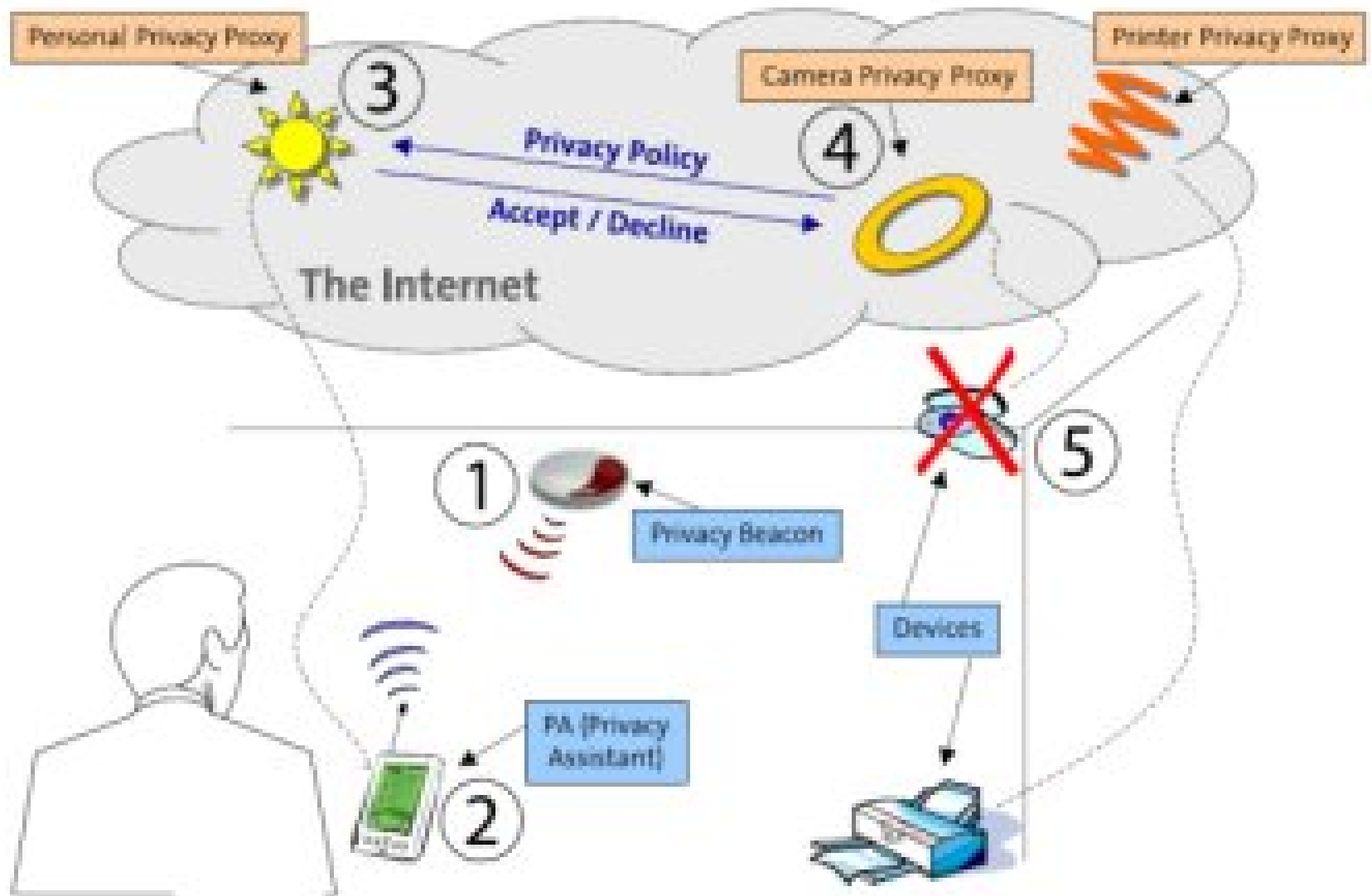
- Feasibility
  - What can be done by technology?
- Convenience
- Communitarian
- Egalitarian

# Social Implications of UBI/Pervasive

- Ubiquity
- Invisibility
- Sensing beyond human range
- Memory amplification

# Principles & Guidelines

- Notice
- Choice & Control
- Anonymity & Pseudo-anonymity
- Proximity & Locality
- Adequate Security
- Access and Recourse
- What people can do
- What technology can do



Overview of Privacy Management System

# Design for What?

- Calls for environmental designers
  - Let's not be left behind!
  - Price of technology vs. buildings
  - Rapid change
- Technology designers are already working on future devices to disappear into buildings, rooms, other artifacts

Ideas about future work

# Interesting Questions

- New challenges for social scientists and designers
- New challenges for computer and other technologists

# Many Interesting Design Questions

- Transparency in social interaction:
  - Conventional tools of self presentation work only for the humans, they have no effect on the data world.
  - The conventional notion of “being alone” is highly problematic (even more than it used to be).
  - What happens when you assume everyone may be recording?
- Design vision must not be not limited to capabilities of humans.
  - *It is critical to understand what a digital system “knows” and can deduce about people and activities.*

# Many Interesting Design Questions

- Anonymity is essentially impossible: technology now exists to automatically recognize individuals
  - from video and audio (and soon from chemical and other “public” traces).
  - Also, almost every object can be identified as well (soon, individual consumer items).
- It is technically easy to correlate many kinds of data, especially about identified individuals and objects
  - No technical limit on where the information might flow

# Design Implications

- Be aware of the far reaching consequences of this issue:
  - if there is no control on information flow, then every space is “visible” to the whole world, potentially including the personal identity of every person who enters the space.
  - “Think before you do”
- Act as advocates for all the interested parties, not just the funding source.

# Ideas for Design

- Unobtrusive but clear indications of the policies in force
  - What monitoring is going on (and where)
  - Where is the information going?
  - How “public” is the wireless node?
- Put the tools in the hands of the workers
  - Provide real choices
  - How can “users” negotiate about these issues with the environment?

# Design Questions

- How would you design a “quiet zone” in a pervasive computing environment
  - Conventional spatial tools (walls, windows, etc.) are not relevant to EM and information flow.
  - look at the full spectrum, not just human senses (e.g., include IR, radio frequencies, chemical details (scent, DNA ID))

# Ideas for Technology

- Need effective means of presenting policies to ordinary users
  - What the environment is doing
  - Where the information goes
  - Who is in charge
  - What are your choices
- How to deploy wireless technology more precisely?
  - Buildings are square, wireless is round!

# A Collaborative Effort

- Social Science and Design can provide sophisticated (and perhaps elegant) ways to build pervasive environments.
- Technologists can provide sophisticated (and perhaps elegant) techniques.
- Together, we may create environments that improve human experience.

# Summary

- Designers should extend ideas from conventional spatial design to implement appropriate policies for digital monitoring
  - Will require creative ideas plus technical developments
- Technologists should focus on critical features, especially, intrusiveness and information sharing
  - Or else the technology will be rejected