# Privacy and Trust: Social Factors

Presented By: David Shelly

# Papers

- Unpacking “Privacy” for a Networked World

  **Leysia Palen and Paul Dourish**

- Privacy Mirrors: Understanding and Shaping Socio-technical Ubiquitous Computing Systems

  **David Nguyen and Elizabeth Mynatt**

# Introduction

- Framework built upon privacy regulation theory
  - Irwin Altman
  - Predates digital technology - people's face-to-face interactions
  - Extended to consider information technology analysis and design

# Introduction

- "*Dialectic and dynamic boundary regulation process*"
  - Dialectic - privacy regulation is conditioned by our own expectations/experiences plus those of others
  - Dynamic – privacy is under continuous negotiation and management
  - Boundary – privacy and publicity are refined according to circumstance

# Introduction

- Privacy concerns
  - Disclosure – audiences are no longer circumscribed by a physical space; space is large, unknown and distant
  - Time (Temporality) – audiences can exist not only in present, but in future as well
  - Identity – we contribute information explicitly and implicitly, both within and without of our direct control

# Altman's Privacy Theory

- Privacy regulation is neither static nor rule-based
- Conceptualizes privacy as the "selective control of access to the self"
- Boundary regulation process
  - "Openness" vs. "Closedness"
  - "Crowding" vs. "Isolation"
- Goal of privacy regulation:
  - Achieve the desired state along this spectrum
- Differences
  - Altman analyzes cultural differences

# Idea of Boundaries

- Move dynamically as context changes
  - Information technology has ability to disrupt and destabilize the regulation of boundaries
- Three boundaries central to characterization of privacy management
  - Disclosure – privacy vs publicity
  - Identity – tensions with audience
  - Temporality – past, present, and future interpretations and actions involving information
- All of the objectives of these boundaries are in tension with each other

# The Disclosure Boundary: Privacy and Publicity

- Retain certain information as private, but also explicitly disclose information
  - Bumper stickers, designer clothing, letters to the editor
- Need to ensure others know something about ourselves
  - Public relations agent needs to make client known
  - In academics – maintain web pages to advertise expertise and request for papers

# The Disclosure Boundary: Privacy and Publicity

- Technology requires disclosure of information simply to be part of it
  - Shopping on-line
- Problems arise when participation is not deliberate
  - Google search – artifacts and traces of past action
  - Public records data
  - Online photographs posted by friends

# The Identity Boundary: Self and Other

- Conventional forms of privacy problems focus solely on the individual
  - Inadequate for privacy
- Affiliation and allegiance need to be considered
  - E-mail signatures with corporate liability
  - Employees discouraged from using corporate email address when posting to public forms

# The Identity Boundary: Self and Other

- *Reflexive interpretability of action*
  - Understanding of our actions will be available or interpretable to others
- Control over how we want to be perceived
  - Web-pages, Usenet postings
- No control over how we want to be perceived
  - Cookie-enabled web page, email distribution list
  - Interpretation in control of recipients and can change with time

# Temporal Boundaries: Past, Present, and Future

- Information disclosure is an outcome of a sequence of historical actions
  - Current actions may affect future situations (academic web page example)
- Future use of information can not always be controlled
  - Nature or format of information should be considered (PDF vs. Microsoft Word)

# Genres of Disclosure

- Genres of disclosure are the result of these boundary tensions
  - Reproduced arrangements of people, technology, and practice that yield meaningful styles of interaction and information
- Violations of these genres
  - Personal information used in ways not originally anticipated
  - Implies an expectation of appropriate use
- Captures relationship between information disclosure and expectation of use

# Case Studies

- Family Intercom
- Shared Calendars
- Active Badges
- Mobile Telephones
- Instant Messaging

# Case Study: Shared Calendars

- Temporal boundary benefits
  - Better coordination by sharing information that was once considered private
- Disadvantages
  - Patterning and sequencing of information
- Impending lay-off example:
  - Employee used online calendar system to discover that every meeting room had been booked all day by Human Resources

# Case Study: Active Badges

- Personal tracking systems based on badges in two labs
  - Central lab - routing phone calls was highly valued
  - Desk-based lab – less useful, intrusive
- Administrative staff vs. Scientific staff
  - Scientific staff – resents technology that would limit their individual freedom and impose greater organizational accountability
  - Admin staff – organizational accountability is already a feature of their working lives
  - Tension between self and other

# Case Study: Instant Messaging

- Temporal boundary tensions
  - Possibility of recording information for future use
- Disclosure boundary
  - IM can advertise publicity and availability to friends
  - Physical space of home keeps IM participation private
- Identity boundary
  - Attention given to who is expected and wanted to be in each of these spaces

# Conclusion

- Conceptual privacy regulation framework
  - Disclosure, Identity, and Temporality boundaries and the tensions that occur with their negotiation
  - Technology disrupts, spans, and establishes these boundaries
- Illuminates specific issues in interaction of privacy and information technology
  - Diverse issues in everyday settings
- Vocabulary for talking about privacy and technology to better understand the impacts of technology

# Privacy Mirrors

- A framework for designing socio-technical ubicomp systems
- Motivation: Address ubicomp dangers
  - Systems collect information and disseminate it inappropriately
  - Systems transmit data without a new user knowing
  - Interfaces don't give users appropriate tools to control and shape the behavior of the system
- Users need to understand capabilities of a system in order to shape the system to meet their needs, practices, and values

# Background

- Ubicomp systems cover three environments:
  - Social
  - Technical
  - Physical
- A change in one effects another
  - Instrument room – changing lights (physical) affects camera performance (technical) and may cause change in usage of system (social)
- A solution in only one environment will not solve privacy issues in ubicomp
- Mirrors – methods *reflect* the history, current state, and nature of socio-technical ubicomp systems

# Privacy Mirrors Framework

- Five characteristics
  - History – of information flow and interactions
  - Feedback – visible representation of history, information, and current state of environment
  - Awareness – provided by feedback
  - Accountability – provided by feedback
  - Change – enacted by users to change system
- Privacy challenges in socio-technical systems is similar to those faced by groupware calendar systems (GCS)
  - *Augur* – GCS used to apply the design of a Privacy Mirror

# History

- Digital technologies can track (log) as many or as few states and interactions as they want
- Want to allow user to understand technical state changes as well as how people interact with that information
  - Gives people greater insight into the social system which they are a part
  - “Hiking trail” – takes time to form
- Augur
  - Logs all accesses as the group shares their calendars
  - Who looked at whose calendar, how often, and from where

# Feedback

- Supports differing cognitive models by providing different levels of information
  - Glance – gives a small amount of information without requiring effort (ex: ambient display)
  - Look – gives more information (ex: information displays showing departures/arrivals)
  - Interact – most amount of information giving greater detail (ex: interactive programs on desktop computers)
- Augur
  - Users know who accessed their calendar, how recently, what was looked at specifically, and from where
  - Want to know if a stranger from another country was accessing their calendar information

# Awareness

- Arises when people process the information presented to them by feedback
  - How they participate
  - How others participate with respect to them
  - How everyone can and can not participate
- Better forms the user's comfort level
  - User can see if their personal comfort level for privacy fits within the current system
- Augur
  - Social - User finds out calendar information is not used by supervisors, but rather by subordinates
  - Technical – Calendar information is not shared until they synchronize their Palm device
  - Physical – Opening a window exposes their calendar

# Accountability

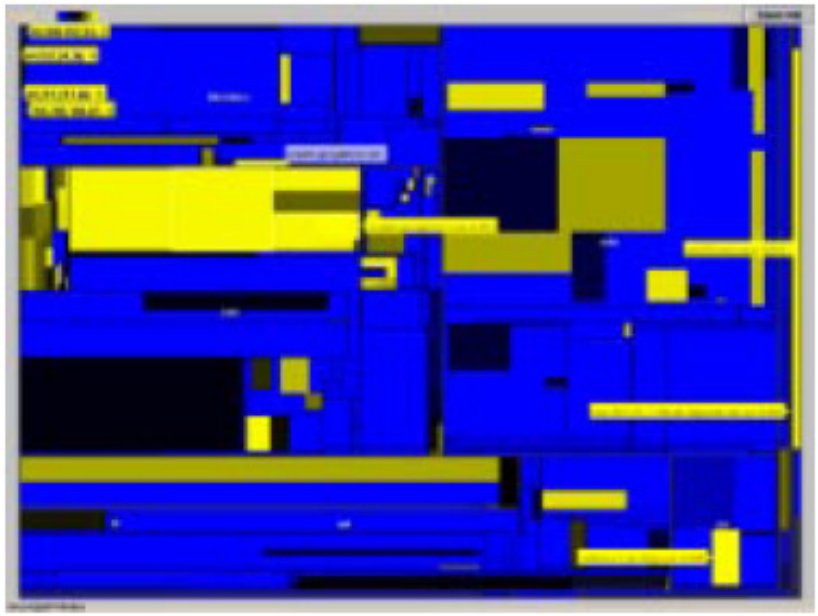
- Plays a large role in social translucence
  - Owner of information should be able to determine who accessed that information
  - Person accessing information should know that their actions have been processed in some way
- "You-know-that-I-know-that-you-know"
- Augur
  - Viewer – Accountability brings in social norms for viewing others calendars
  - Owner – Knowing who and how often someone looks at your calendar can change your comfort level for sharing calendar information

# Change

- User should be able to utilize information to form awareness
  - Aware of a beneficial flow of information – may want to provide more information into flow
  - Aware of an unhelpful flow of information – may want to stop flow, restrict flow, or modify the information involved in the flow
- By understanding the system the user can change technical, social, and physical settings to better their needs
- Augur
  - Technical - User can change the permissions of those accessing their calendar information
  - Social – Change descriptions of appointments

# Web Server Log Mirror (WSLM)

- Uses Treemaps to visualize pertinent information that is normally invisible
- Divided by domain and host name, and again by sub-domains until a specific machine occupies a single rectangle
- Size – determined by number of hits coming from a specific machine
- Color – More current visits (yellow), two or more weeks old (bright blue)



# Web Server Log Mirror (WSLM)

- History
  - Shown by size and color
  - Example: large rectangle and middle shade shows that gigan.cc.gatech.edu accessed site many times about a week ago
  - Can not view distribution of accesses using interface
- Feedback
  - Also shows which machine accessed web site and which particular page was accessed
  - Glance (color patterns), look (specific domains), interact (activity of specific machine)
  - Does not tell users they are logging them however

# Web Server Log Mirror (WSLM)

- Awareness
  - Large number of accesses to pages which started with "/script"
  - Learned that web server worms were trying to exploit security holes in "/script" file
  - Many people from different countries visited
  - Search engines crawled site many times a day
- Accountability
  - Logs host names and IP addresses
  - However, not easy to connect person with a hostname
  - Does not tell visitors that web page owners can see what they are viewing
  - "You-know-that-I-know-that-you-know" not created

# Web Server Log Mirror (WSLM)

- Change
  - Better understanding of system after several weeks of use
  - Social – change content of site
  - Technical – add passwords
  - Do nothing – see if behavior changes

# Conclusion

- Privacy Mirrors allow users to:
  - Enact change and see the feedback reflect back to them
  - Understand the system better by revealing its capabilities and constraints
  - Understand the actions of others since access to information is tracked adding accountability
  - Make sense of their environment, (social, technical, and physical) giving users comfort and confidence in socio-technical systems
- Brings “physics” to ubiquitous computing