PRIVACY IN PERVERSIVE COMPUTING
Marc Langheinrich
ETH Zurich, Switzerland

Approaches to Ubicomp Privacy
Disappearing Computer Troubadour Project (10/2002 - 05/2003)

- Promote Absence of Protection as User Empowerment
  - “It’s maybe about letting them find their own ways of cheating”
- Make it Someone Else’s Problem
  - “For [my colleague] it is more appropriate to think about [security and privacy] issues. It’s not really the case in my case”
- Insist that Good Security will Fix It
  - “All you need is really good firewalls”
- Conclude it is Incompatible with Ubiquitous Computing
  - “I think you can’t think of privacy… it’s impossible, because if I do it, I have troubles with finding [a] Ubicomp future”

Today’s Menu

- Understanding Privacy
  - Definitions
    1. Public policy
    2. Laws and regulations
    3. Interpersonal aspects
- Technical Approaches
  - Challenges
    1. Location privacy
    2. RFID privacy
    3. Smart environments
What Is Privacy?

- “The right to be let alone.”
  - Warren and Brandeis, 1890 (Harvard Law Review)
- “Numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the housetops’”

Technological Revolution, 1888

The KODAK CAMERA

100 Instantaneous Pictures!

Anybody can use it. No knowledge of photography is necessary.

The latest and best outfit for amateurs.

Send for descriptive circular.

Price $25.00.

The Eastman Dry Plate & Film Co.
Rochester, N.Y.

1888
Information Privacy

• “The desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others.”
  • Alan Westin, 1967
    Privacy And Freedom, Atheneum
Why Privacy?

- “A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organizations to intrude on that autonomy... privacy is a key value which underpins human dignity and other key values such as freedom of association and freedom of speech...“
  - Preamble To Australian Privacy Charter, 1994
- “All this secrecy is making life harder, more expensive, dangerous and less serendipitous”
  - Peter Cochrane, Former Head Of BT Research
- “You have no privacy anyway, get over it“
  - Scott McNealy, CEO Sun Microsystems, 1995

Informational Self-Determination

“Informationelle Selbstbestimmung”

- “If one cannot with sufficient surety be aware of the personal information about him that is known in certain part of his social environment, ... can be seriously inhibited in his freedom of self-determined planning and deciding. A society in which the individual citizen would not be able to find out who knows what when about them, would not be reconcilable with the right of self-determination over personal data. Those who are unsure if differing attitudes and actions are ubiquitously noted and permanently stored, processed, or distributed, will try not to stand out with their behavior. ... This would not only limit the chances for individual development, but also affect public welfare, since self-determination is an essential requirement for a democratic society that is built on the participatory powers of its citizens.”

  *German Federal Constitutional Court (Census Decision ’83)*
Informational Self-Determination
“Informationelle Selbstbestimmung”

- “The problem is the possibility of technology taking on a life of its own, so that the actuality and inevitability of technology creates a dictatorship. Not a dictatorship of people over people with the help of technology, but a dictatorship of technology over people.”
- Ernst Benda (1983)
  Federal Constitutional Court Chief Justice
Privacy Law History

- Justices Of The Peace Act (England, 1361)
  - Sentences for Eavesdropping and Peeping Toms
- "The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail; its roof may shake; ... – but the king of England cannot enter; all his forces dare not cross the threshold of the ruined tenement"
  - William Pitt the Elder (1708-1778)
- First Modern Privacy Law in the German State Hesse, 1970

Fair Information Principles (FIP)

- Drawn up by the OECD, 1980
  - "Organisation for economic cooperation and development"
  - Voluntary guidelines for member states
  - Goal: Ease transborder flow of goods (and information!)
- Five Principles (simplified)
  1. Openness
  2. Data access and control
  3. Data security
  4. Collection Limitation
  5. Data subject’s consent
- Core principles of modern privacy laws world-wide
Laws and Regulations

- Privacy laws and regulations vary widely throughout the world
- US has mostly sector-specific laws, with relatively minimal protections
  - Self-Regulation favored over comprehensive Privacy Laws
  - Fear that regulation hinders e-commerce
- Europe has long favored strong privacy laws
  - Often single framework for both public & private sector
  - Privacy commissions in each country (some countries have national and state commissions)

EU Privacy Law

- Data Protection Directive 1995/46/EC
  - Sets a Benchmark For National Law For Processing Personal Information In Electronic And Manual Files
  - Follows OECD Fair Information Practices
  - Facilitates Data-flow Between Member States And Restricts Export Of Personal Data To „Unsafe“ Non-EU Countries
  - Provisions for “public electronic communications services“
- Data Retention Directive 2006/24/EC
  - Orders storage of “traffic data“ for law enforcement
Safe Harbor

  - US companies self-certify adherence to requirements
  - Dept. of Commerce maintains list (1429 as of 04/08)
    http://www.export.gov/safeharbor/
- Signatories must provide
  - notice of data collected, purposes, and recipients
  - choice of opt-out of 3rd-party transfers, opt-in for sensitive data
  - access rights to delete or edit inaccurate information
  - security for storage of collected data
  - enforcement mechanisms for individual complaints
- Approved July 26, 2000 by EU
  - reserves right to renegotiate if remedies for EU citizens prove to be inadequate

Privacy in Pervasive Computing

3. INTERPERSONAL PRIVACY
Privacy Invasions

- When Do We Feel that Our Privacy Has Been Violated?
  - Perceived privacy violations due to crossing of “privacy borders”
- Privacy Boundaries
  1. Natural
  2. Social
  3. Spatial / temporal
  4. Transitory

Privacy Borders (Marx)

- Natural
  - Physical limitations (doors, sealed letters)
- Social
  - Group confidentiality (doctors, colleagues)
- Spatial / Temporal
  - Family vs. work, adolescence vs. midlife
- Transitory
  - Fleeting moments, unreflected utterances
Privacy Regulation Theory

- Privacy as Accessibility Optimization: Inputs and Outputs
  - Spectrum: “Openness”/ “Closedness”
  - Contrasts with privacy as withdrawal (“to be let alone“)
  - Privacy not monotonic: “More” is not always “better”
- Dynamic Boundary Negotiation Process
  - Neither static nor rule-based
  - Requires fine-grained coordination of action & disclosure
  - Focus on public spaces, mediated by spatial environment

Managing Privacy Boundaries

- Use Altman’s Theory for Networked Environments
  - Very different from real-world public spaces!
- Disclosure Boundary: Private and Public
  - We sometimes need publicity to limit accessibility
- Identity Boundary: Self and Other
  - Acting according to status, group, affiliation
  - Disclosure according to recipient’s identity & role
  - Disclosure as means to differentiate or associate
- Temporality Boundary: Past, Present, and Future
  - Effects of temporal sequence of disclosures
Today’s Menu

Understanding Privacy
- Definitions
  1. Public policy
  2. Laws and regulations
  3. Interpersonal aspects

Technical Approaches
- Challenges
  1. Location privacy
  2. RFID privacy
  3. Smart environments

Privacy in Pervasive Computing
TECHNICAL APPROACHES
The Information Society

- “More transactions will tend to be recorded, the records will tend to be kept longer, information will tend to be given to more people, more data will tend to be transmitted over public communication channels, fewer people will know what is happening to the data, the data will tend to be more easily accessible, and data can be manipulated, combined, correlated, associated and analysed to yield information which could not have been obtained without the use of computers.”

Ubicomp Privacy Implications

- Data Collection (“more transactions“)
  - Scale (everywhere, anytime)
  - Manner (inconspicuous, invisible)
  - Motivation (context!)
- Data Types (“not without computers“)
  - Observational instead of factual data
- Data Access (“more easily accessible“)
  - “The Internet of Things“
FIP Challenges in Ubicomp

- How to inform subjects about data collections?
  - Unintrusive but noticeable
- How to provide access to stored data?
  - Who has it? How much of this is “my data“?
- How to ensure confidentiality, and authenticity?
  - Without alienating user!
- How to minimize data collection?
  - What part of the “context“ is relevant?
- How to obtain consent from data subjects?
  - Missing UIs? Do people understand implications?

Border Crossings in Ubicomp

- Smart appliances (natural borders)
  - “Spy“ on you in your own home
- Family intercom (social borders)
  - Grandma knows when you’re home
- Consumer profiles (temporal borders)
  - Span time & space
  - “Memory amplifier“ (transitory borders)
    - Records careless utterances
Location Privacy

• “... the ability to prevent other parties from learning one’s current or past location.” (Beresford and Stajano, 2003)

• Why Share Your Location?
  • By-product of positioning technology (e.g., cell towers)
  • Required to use service (recommendations, toll roads, ...)
  • Let others (friends, family) know where I am

• Why NOT to Share Your Location?
  • Current & past location reveal activities, interests, identity
Location Privacy Technology

- Many Proposals
  - Laws/regulations and audits (enterprise privacy)
  - Anonymization (“k-anonymity“)
  - Obfuscation
  - Rule-based access control
- Privacy Model?
  - Assumption: Less location disclosure means more privacy

(Krumm, 2008) Provides Overview of State-of-the-Art

Location Obfuscation

- Adding noise, perturbation, dummy traffic to location data
  - Protects against attackers, but degrades service use
  - (Krumm, 2007) showed that LOTS of obfuscation is needed
  - Typically combined with rules to selectively adjust accuracy
Location Mix Zones

- Frequently Change Pseudonyms to Prevent Tracking
  - Change often trivial to detect
- Idea: Designate “Mix Zones” With No Tracking / LBS Active
  - Change pseudonyms only within mix zone
  - (Beresford and Stajano, 2003) offer probabilistic model for unlinkability in mix zones
RFID Privacy Concerns

Why RFID Privacy?

- Embarrassment
  - Whig? Underwear? Medicine?
- Criminal Acts
  - Theft, assault, murder, terror

Passport
  - Name: John Doe
  - Nationality: USA
  - Visa for: Israel

Wallet
  - Cash: 370 Euro
  - Student ID: #2845/ETH

Viagra
  - Maker: Pfitzer
  - Size: Maxi (60 pills)

Tiger Tanga
  - Maker: Aldi
  - Last washed: 5 days ago
Why RFID Privacy?

- Embarrassment
  - Whig? Underwear? Medicine?
- Criminal Acts
  - Theft, assault, murder, terror
- Indirect Control
  - Subtle influence through consumer profiles
- Direct Control
  - “Technology Paternalism”, government surveillance


RFID Privacy Approaches

- Tag Deactivation
  - Fry, cut, or silence (software)
  - Prevents further use
- Tag Encryption (Lots!)
  - More expensive tags
  - Password management!
- Readout Interference (“Blocker-Tag”, “Guardian”)
  - Reliability? Feasibility? Legal?
  - Burdens user (conscious use, configuration)
- (Juels, 2006) Provides Overview of State-Of-The-Art
  - See also (Langheinrich, 2008) or (Spiekermann, 2008)
Shamir Tags: “Keyless“ Encryption

- Idea: Encrypted Tag Carries Its Own Key
  - No need to manage keys!
- Prevent Skimming: Key Readout Takes Long Time
  - Bitwise release, short range (e.g., one bit/sec)
  - Intermediate results meaningless, since encrypted
- Prevent Tracking: Reply With Random Bits
  - Decryption requires all bits being read
- Allow Known Tags to be Directly Identified
  - Allows owner to use tags without apparent restrictions
  - Initial bit-release enough for instant identification from known set

Smart Environments

- Privacy Middleware
  - Machine-readable privacy policies control data collection, processing, access
  - Personal device (e.g., mobile phone) to monitor and configure environment
  - Optional: Built-in data obfuscation
- Example Projects
  - PawS/P3P (Langheinrich, 2003)
  - Confab toolkit (Hong and Landay, 2004)

Presence Technology

- Providing Control and Awareness to Users
  - Who is seeing what information about me?
- CSCW / Telecommuting
  - (Bellotti and Sellen, 1993) – EuroPARC’s RAVE media space
  - (Neustaedter, Greenberg, and Boyle, 2006) – Blurring?
- Location Disclosure
  - (Hong and Landay, 2004) – Lemming: Location-enhanced IM
  - (Consolvo et al., 2005) – Social relations and loc. disclosure
Related Issues

- Privacy and Usability
  - CUPS group @ CMU
- Hippocratic Databases
  - Privacy-compliant processing
- Statistical Databases
  - Anonymization in databases ("k-anonymity")
- Economics of Privacy
  - When do people share data?
Take Home Message

- Privacy is Not Just Secrecy and Seclusion!
  - Privacy is a process, not a state
  - Solution requires good understanding of social, legal, and policy issues involved
- Pervasive Computing Offers New Challenges
  - Invisible, comprehensive, sensor-based, ...
- UbiComp (Privacy) Challenges
  - User interface (notice, choice, consent)
  - Protocols (anonymity, security, access)
  - Social compatibility (privacy boundaries)

Some Techno Fallacies

- The Objectivity Of Numbers
- Data Means Knowledge
- More Data Means More Knowledge
- If It Is In The Computer, It Must Be Right
- If You Have Nothing To Hide, There’s No Danger
- Less Data Means More Privacy

Technology Is Neither Good Nor Bad. Nor Is It Neutral

Thank You For Your Attention

• Understanding Privacy
  • Definitions
  1. Public policy
  2. Laws and regulations
  3. Interpersonal aspects

• Technical Approaches
  • Challenges
  1. Location privacy
  2. RFID privacy
  3. Smart environments

General Reading

  http://codev2.cc/
Privacy Law

- Privacy & Human Rights 2006. EPIC

Privacy and Technology