Personal Privacy in Ubiquitous Computing

Marc Langheinrich
ETH Zurich, Switzerland

http://www.inf.ethz.ch/~langhein/
What’s Up?

- What is privacy, anyway?
  - Privacy definitions
  - Privacy motivation
- How is privacy changing?
  - Privacy evolution
  - Privacy threats
- How can we achieve privacy?
  - Privacy solutions
1. Definitions and Motivations

What is Privacy, Anyway?

1. What is Privacy?
   Definitions and Motivation

2. How is Privacy Changing?
   Evolution and Threats

3. How can We Achieve Privacy?
   Concepts and Solutions
What Is Privacy?

- „The right to be left alone."
  - Louis 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’”

Louis D. Brandeis, 1856 - 1941
What Is 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“)
Facets

- Informational privacy
  - Personal data (name, address, hobbies, ...)

- Privacy of communications
  - Phone calls, (e-)mail, ...

- Territorial privacy
  - Privacy of your home, office, ...

- Bodily privacy
  - Strip searches, drug testing, ...
Functional Definition

Privacy invasive effects of surveillance and data collection due to crossing of personal borders
  – Prof. Gary T. Marx, MIT

Privacy boundaries
  – Natural
  – Social
  – Spatial / temporal
  – Transitory
Examples: Border Crossings

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

Privacy Litmus-test: What borders can be crossed?
Privacy History

- Justices of the peace act (England, 1361)
- „The poorest man may in his cottage bid defiance to all the force of the crown”
  - William Pitt, English Parliamentarian, 1765
- 1948 United Nations: Universal declaration of human rights, article 12
  - No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honor or reputation.
- 1970 European convention on human rights, article 8
- First data protection law of the world: state of Hesse, Germany (1970)
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
Driving Factors

- As empowerment
  - “Ownership” of personal data
- As utility
  - Protection from nuisances (e.g., spam)
- As dignity
  - Balance of power (“nakedness”)
- As constraint of power
  - Limits enforcement capabilities of ruling elite
- As by-product
  - Residue of inefficient collection mechanisms

Example: Search And Seizures

- 4\textsuperscript{th} amendment of US constitution
  - “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

- Privacy as utility? Privacy as dignity?
All home software configured by law to monitor for illegal activities
- Fridges detect stored explosives, PCs scan hard disks for illegal data, knifes report stabbings

Non-illegal activities NOT communicated
- Private conversations, actions, remain private
- Only illegal events reported to police

No nuisance of unjustified searches
- Compatible with 4th amendment?
2. Evolution and Threats

How is Privacy Changing?

1. What is Privacy?
   Definitions and Motivation

2. How is Privacy Changing?
   Evolution and Threats

3. How can We Achieve Privacy?
   Concepts and Solutions
Collection Parameters

1. Scale
   - To what extend is my life visible to others?
2. Manner
   - How obviously is data collected?
3. Type
   - What type of data is recorded?
4. Motivation
   - What are the driving factors?
5. Accessibility
   - How does one find anything in this data?
1. Collection Scale

- Before: public appearances
  - Physically separated in space and time
- Today: online time
  - Preferences & problems (online shopping)
  - Interests & hobbies (chat, news)
  - Location & address (online tracking)
- Tomorrow: the rest
  - Home, school, office, public spaces, ...
  - No switch to turn it off?
2. Collection Manner

- Before: reasonable expectations
  - You see me – I see you

- Today: visible boundaries
  - Online, real-world electronic transactions

- Tomorrow: invisible interactions
  - Interacting with a digital service?
    - Life recorders, room computers, smart coffee cups
  - No blinking „recording now“ LED?
3. Collection Types

- Before: eyes & ears
- Today: electrical and digital surveillance tools
- Tomorrow: better sensors
  - More detailed & precise data
  - Cheaper, smaller, self-powered (ubiquitous!)
- Do I know myself best?
  - Body sensors detect stress, anger, sadness
  - Health sensors alert physician
  - Nervous? Floor & seat sensors, eye tracker
4. Collection Motivation

- Before: collecting out-of-ordinary events
- Today: collecting routine events
- Tomorrow: smartness through pattern prediction
  - More data = more patterns = smarter
  - Context is everything, everything is context
- Worthless information? Data-mining!
  - Typing speed (dedicated?), Shower habits (having an affair?), Chocolate consumption (depressed?)
5. Collection Accessibility

- Before: natural separations
  - Manual interrogations, word-of-mouth
- Today: online access
  - Search is cheap
  - Database federations
- Tomorrow: cooperating objects?
  - Standardized semantics
  - What is my artifact telling yours?
  - How well can I search your memory?
Virtual Dad

- Road Safety International sells “black box” for car
  - Detailed recording of position (soon), acceleration, etc.
  - Audio warnings when speeding, cutting corners
  - Continuous reckless driving is reported home
- Sold as piece of mind for parents
  - “Imagine if you could sit next to your teenager every second of their driving. Imagine the control you would have. Would they speed? Street race? Hard corner? Hard brake? Play loud music? Probably not. But how do they drive when you are not in the car?”

Source: http://www.roadsafety.com/Teen_Driver.htm
### Car Monitoring

- **ACME rent-a-car, new jersey**
  - Automatically fines drivers US$150,- at speeds over 79mph
  - GPS records exact position of speed violation

- **Autograph system**
  - Pilot program 1998/99, houston, TX
  - Insurance based on individual driving habits (when, where, how)
  - GPS tracking, mobile communication, data center

*Source: [Insurance & Technology Online, Jan 2nd 2002](http://www.insurancetech.com/story/update/IST20020108S0004)*

Other Examples

- Electronic toll gates
- Consumer loyalty cards
- Electronic patient data
- Computer assisted passenger screening (CAPS)
  - Improved systems in the works (post 9/11)
  - Plans: link travel data, credit card records, address information, ...
3. Concepts and Solutions

How can We Achieve Privacy?

1. What is Privacy? Definitions and Motivation
2. How is Privacy Changing? Evolution and Threats
3. How can We Achieve Privacy? Concepts and Solutions

January 20, 2003
Fair Information Principles

- Organization for economic cooperation and development (OECD), 1980
- Voluntary guidelines for members to ease international flow of information (simplified):

1. Notice & disclosure
2. Choice & consent
3. Anonymity & pseudonymity
4. Data security
5. Access & recourse
6. Meeting expectations
1. Notice And Disclosure

- No hidden data collection!
  - Legal requirement in many countries
- Established means: privacy policies
  - Who, what, why, how long, etc. ...

- How to publish policies in Ubicomp?
  - Periodic broadcasts
  - Privacy service?
- Too many devices?
  - Countless announcements an annoyance
2. Choice & Consent

- Participation requires *explicit consent*
  - Usually a signature or pressing a button
- True consent requires *true choice*
  - More than „take it or leave it“

- How to ask without a screen?
  - Designing UI‘s for embedded systems, or
  - Finding means of delegation (is this legal?)

- Providing conditional services
  - Can there be levels of location tracking?
3. Anonymity, Pseudonymity

- Anonymous data comes cheap
  - no consent, security, access needed
- Pseudonyms allow for customization
  - user can discard at any time

- Sometimes one cannot hide!
  - No anonymizing cameras & microphones
- Real-world data hard to anonymized
  - Even pseudonyms can reveal true identity
4. Security

- No one-size-fits-all solutions
  - High security for back-end storage
  - Low security for low-power sensors
- Real-world has complex situation-dependant security requirements
  - Free access to medical data in emergency situations
- Context-specific security?
  - Depending on device battery status
  - Depending on types of data, transmission
  - Depending on locality, situation
5. Access & Recourse

- Identifiable data must be accessible
  - Users can review, change, sometimes delete
- Collectors must be accountable
  - Privacy-aware storage technology?
- Ubicomp applications like lots of data
  - Increased need for accounting and access
- Carefully consider what is relevant
  - How much data do I really need?
6. Meeting Expectations

- Ubicomp: *invisibly* augments real-world
- Old habits adapt slowly (if ever)
  - People expect solitude to mean privacy
  - Strangers usually don’t know me
- No spying, please (Proximity)
  - Devices only record if owner is present
- Rumors should not spread (Locality)
  - Local information stays local
  - Walls and Flower-Pots can talk (but won’t do so over the phone)
Privacy Tools

- Technical
  - Encryption & authentication
  - Anonymity & pseudonymity
  - Transparency & trust
- Legal
  - Laws and regulation
- Social
  - Ethics & social norms
Laws and Regulations

- US has mostly sector-specific laws, with relatively minimal protections
  - Differentiates between public and private sector
  - Self-regulation for private sector (companies)
  - Fear that regulation hinders e-commerce
- Europe has long favoured strong privacy laws
  - Often single framework for both public & private sector
  - Privacy commissions in each country (some countries have national and state commissions)
US Private Sector Laws

- Fair Credit Reporting Act, 1971, 1997
- Cable TV Privacy Act, 1984
- Video Privacy Protection Act, 1988
- Health Insurance Portability And Accountability Act, 1996
- Children’s Online Privacy Protection Act, 1998
- Gramm-leach-bliley-act (Financial Institutions), 1999
EU Data Directive

1995 Data Protection Directive 95/46/EC
- Sets a benchmark for national law for processing personal information in electronic and manual files
- Follows OECD fair information practices
  - Collection limitation, openness, purpose specification, use limitation, access, security, participation, accountability
- Facilitates data-flow between member states
- Restricts export of personal data to „unsafe“ non-EU countries
  - Safe harbor agreement with US
Post 9-11 Issues (EU)

- Directive on Privacy and Electronic Communications 2002/58/EC
  - Members states have until 11/03 to implement national law allowing traffic data retention
  - Retention period: 12 months – 7 years (proposal)

- Data to be Retained (Planned Requirement):
  - Email: IP address, message ID, sender, receiver, user ID
  - Web/FTP: IP address, User ID, Password, Full Request
  - Phone: numbers called (whether connected or not), date, time, length, geographical location for mobile subscribers

See also: http://www.epic.org/privacy/intl/data_retention.html
Watching The Watchers

- Mutually Assured Surveillance
  - All Have Access To (Almost) All Data
- Reciprocal Accountability
  - Restaurant Analogy: No One Openly Stares
- “An Armed Society Is A Polite Society”  
  - John Campell, 1940

David Brin: The Transparent Society

- Reason: There Are No Secrets For The Powerful
  - Secrecy And Privacy Protects Only Elite
Summary & Outlook
The Take-Home Message

1. What is Privacy?
   Definitions and Motivation

2. How is Privacy Changing?
   Evolution and Threats

3. How can We Achieve Privacy?
   Concepts and Solutions
Defining Privacy

- Different facets
  - Informational, communication, territorial, bodily

- Border crossings
  - Natural, social, spatial/temporal, transitional

- Different motivations
  - Empowerment, dignity, utility, constrain of power, by-product

- Not limitless
  - Accountability important part of social fabric
Solution Space

Inspired by OECD fair information practices
- Notice & disclosure
- Choice & consent
- Security

Interdependencies
- Technical possibilities
- Legal requirements
- Social issues

Access & Control
Recourse
Meeting Expectations*
The Take Home Message

- Many questions, few answers
  - Technology, laws still to evolve
- Ubicomp adds a new quality to privacy
  - Invisible, real-world coverage, comprehensive collection, inconspicuous
- Ubicomp (privacy) challenges
  - User interface (notice, choice, consent)
  - Protocols (anonymity, security, access, locality)
  - Social acceptance (user expectations)
Recommended Reading

More Books

- Security for Ubiquitous Computing, by Frank Stajano
- Privacy & Human Rights, EPIC
Privacy Web Sites

- http://www.privacyinternational.org
- http://www.privacyfoundation.org
- http://www.privacyexchange.org
- http://www.privacycouncil.com
- http://www.privacyplace.com
- http://www.junkbusters.com
- http://www.privacilla.org
- http://www.statewatch.org
- http://www.privacy.org
- http://www.pandab.org
- http://www.epic.org
- http://www.cdt.org
Points for Discussion

Macro Level
- Technological vs. legal, social solutions
- Balance between safety & privacy
- Life better without privacy?

Micro Level
- Data requirements of Ubicomp apps
- Storage & profiling, providing user access
- Privacy as part of design process