The DC Privacy Troubadour

Assessing Privacy Implications of DC-Projects

Marc Langheinrich
Swiss Institute of Technology (ETH)
Zurich, Switzerland

www.inf.ethz.ch/~langhein
Outline

- DC privacy troubadour action
  - Project history and goals
  - Visits: overview and findings
- First steps to Ubicomp-privacy
  - Prescribing privacy: troubadour implications
  - Assessing privacy: privacy borders
  - Realizing privacy: pawS
- My two cents
Troubadour History

- Initial meetings 10/01 and 01/02
  - Privacy workshop (about 12 participants)
  - Members from three DC groups
  - Goal: project privacy assessment
  - Proved difficult

- Troubadour application 05/02
  - Visits to up to 10 projects (in two rounds)
  - Goal: learn about technical details
  - Goal: get feedback directly from developers

Leads to “real-world” privacy guidelines
Troubadour Specs

- 7 visits in 6 months
  - 10/02 Ambient Agoras (EDF Paris, France)
  - 11/02 Smart-Its (Univ. Lancaster, UK)
  - 12/02 Oresteia (King’s College, London, UK)
  - 01/03 Smart-Its (Gothenburg Univ., Sweden)
  - 02/03 E-Gadgets (CTI Patras, Greece)
  - 05/03 Ambient Agoras (EDF Paris, France)
  - 05/03 Interliving (Univ. de Paris-Sud, France)

- Out: Seminars, lectures, workshops
- In: Interviews (~6 hours), videos, pictures, text
Results?

- Different national attitudes to privacy
  - Political histories vary widely in Europe
- Different personal attitudes to privacy
  - Concerned but optimistic (solvable)
  - Concerned but pessimistic (unsolvable)
  - Unconcerned (no moral responsibility)
  - Unconcerned (trivial problem)
- Bottom line: no thoughts on privacy!!
  - not now (maybe later...)
  - Troubadour goals revised: Not “What”, but “Why”? 
Detailed Comments I

- Concerned but optimistic (solvable)
  - No time to think about: Troubadour agenda items and interviews get cut short or pushed off meeting schedule... (there’s more important work to do!)
  - Not beneficial to think about: “I find it a bit strange to already as a designer react to it before even, somehow, we could see it. somehow it also destroys this, you know, sort of, like, creativity...”
Detailed Comments II

- Concerned but pessimistic (unsolvable)
  - Too early to think about (prototypes): “we first thought: let’s build this first…”
  - Too difficult to think about: “I think you can't think of privacy when you are trying out... it's impossible, because if I do it, I have troubles with finding [a] Ubicomp future [laughs]”
  - A fight that will be lost: “you will probably develop some laissez-faire. your personal data will get out of control”
Detailed Comments III

- Unconcerned (no moral responsibility)
  - Not my job: “for [my colleague] it is more appropriate to think about privacy issues. it is not really the case in my case.”
  - Will get sorted out by society: “little by little – I expect that would be a process of 20 years – that you need a generation actually to sort out, where is the social value, [...] and then formalize the legislation”
Detailed Comments III

DC-Tales, Greece

- Unconcerned (no moral responsibility)
  - Will get sorted out by society: “it's maybe about letting them find their own ways of cheating, you know, and letting them, you know... this is maybe where their part comes in: letting them find their own ways of cheating, abusing, or, you know, making a fool out of each other. but they can really design these kind of really bad things if you want themselves, rather than, kind of, you know, doing it secretly”
Detailed Comments IV

- Unconcerned (trivial problem)
  - Problem (security issues) solved already: “I think all you need is really good firewalls. [...] if you know, or if you are aware of, that this might be a problem, then you are safe.”
  - Smart users will figure it out: “all you need is to be able to configure your own network within an existing structure... we will get better at hacking it, and so [you can] change your history.”
Results?

- Different national attitudes to privacy
  - Political histories vary widely in Europe

- Different personal attitudes to privacy
  - Concerned but optimistic (solvable)
  - Concerned but pessimistic (unsolvable)
  - Unconcerned (no moral responsibility)
  - Unconcerned (trivial problem)

- Bottom line: no thoughts on privacy!!
  - not now (maybe later...)
  - Troubadour goals revised: Not “What”, but “Why”?
Prescribing Privacy?

- Putting privacy on critical path
  - Project output: demos, prototypes, papers
  - Easier to develop without privacy!
  - Possible to develop without privacy!
  - Integral part of EU project applications?

- Providing privacy measurements
  - Simple privacy-tests necessary
  - Generic privacy-toolbox useful
Assessing Privacy

- Question: When do I feel that my privacy has been violated?
- Answer: When personal borders get crossed
  - Prof. Gary T. Marx, MIT
- Privacy boundaries
  - Natural
  - Social
  - Spatial / temporal
  - Transitory
Privacy Boundaries

- Natural
  - Physical Limitations (Doors, Sealed Letters)
- Social
  - Group Confidentiality (Doctors, Colleagues)
- Spatial / Temporal
  - Family vs. Work, Adolescence vs. Midlife
- Transitory
  - Fleeting Moments, Unreflected Utterances
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?
Realizing Privacy: pawS

Privacy Proxies

Privacy Beacons

Privacy DB

Privacy Policy
Accept / Decline

DC-Tales, Greece

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
U-Privacy: My Two Cents

- Not the (DC) developers fault
  - Privacy unlike energy, size (i.e., ignorable)
  - Nobody asks for it (really)
  - No one knows where to start

- Tools, incentives needed!
  - Guidelines for privacy (where to start)
  - Tools (technical) for privacy (like energy)
  - Money for privacy (asking for it)
1. Privacy Beacons

- Let people (data subjects) know about collection
  - “Software” beacons as part of service discovery
  - “Stand-alone” beacons for video, audio rec.

- Beacons describe data to be collected, purpose
  - Machine-readable privacy policies (P3P)
  - Extended with ubicomp-specific fields
2. Privacy Proxies

- Service proxy solicits data subject’s consent
  - User proxy compares preferences (APPEL) with policy obtained from service proxy
- Provide single entry point for data exchange
  - Allows automated data inspection, update, deletion
3. Privacy Aware Database

- Store personal info together with P3P policy
  - Data and policy (metadata) form single logical unit
- Requires usage policy for each data access
  - DB compares policies for data subject and data user and only releases records w/ matching policies
  - Each data usage recorded in usage log (auditing)