mobile business

Addressing the Privacy Paradox by Expanded Privacy Awareness – The Example of Context Aware Services

IFIP PrimeLife Summer School 2009
September 9, 2009

André Deuker
Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe-University Frankfurt

ifip PrimeLife

Motivation

Some connections:

- facebook safebook Monolithic vs. Distributed Design
  - Who is willing to pay for privacy?
  - Who is willing to pay for services?

Business Perspective

- Legal Regulation & Economic Incentives
- Privacy in Business Models

→ Development of an artefact to support privacy in business models for context aware services.

PrimeLife ifip

Privacy Protection in Context Aware Services

*"Demands for personal data are teaching people to be obstructionists. When dealing with organisations, it is **best for them to obfuscate and lie in order to protect their private sphere**"* *(Roger Clarke, Business Cases for PETs)*

Context Aware Services are **based on information about their users** as e.g. time, position, and interests.

Privacy Protection Aspects of minor importance and **not part of the value approach** of most business models for context aware services.

Demand for Privacy and the Privacy Paradox

Privacy Paradox: *Discrepancy between users privacy needs formulated on an abstract level and their actual behaviour of interaction with context aware services.*

↓

Utility $\leqq$ Benefit – Costs

→ Monetary Costs

→ Risks

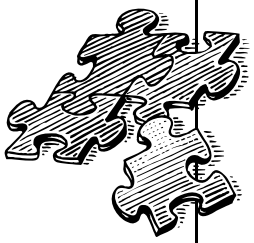
} Systematic under-assessment of costs; biased decision

- Users have to be enabled to fully assess costs that are related the usage of context aware services.
- Demand for privacy preserving mechanisms is (artificially) lower than it should be (?)

mobile business

3 Dimensions of the Privacy Paradox

- **Incomplete Information**
  - Incomplete Information about disclosed data
  - Incomplete information about consequences of disclosed data



- **Bounded Rationality**
  - Wrong or biased conclusions in spite of complete information

- **Psychological Factors**
  - Users draw less attention to privacy risks than to other types of risk
  - Immediate gratification can influence users' risk perception

Raising Privacy Awareness to address the privacy paradox

Privacy Awareness:

Awareness of what data is disclosed and what consequences/risks this might bear.

A precondition for the employment of PETs:

- Identification of risks
- Assessment of risks

→ Users need to be motivated to address their own limits of risk perception.

How to Raise Privacy Awareness?

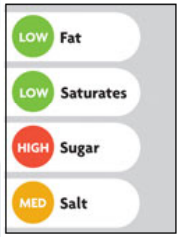
On a general level:

- Tutorials, Talks, Campaigns

On an application level:

- Before using the service
- While using the service

→ **Informing & Warning**



Challenges for Privacy Awareness on an Application Specific Level

Technical: How can/should privacy awareness be integrated in context aware services?

Organisational: Can privacy awareness be integrated into business models?

- More parties involved than in the process of raising application independent privacy awareness.
- Interests of all involved parties have to be considered and harmonised
- Legal Obligation vs. Economic Incentive

cash flow, retention rate (switching costs), data

Incentives to establish application specific context awareness

Users will provide less, or incomplete information when they are concerned about their privacy.

Theory of Reactance:

- Emotional over reaction with regard to a presented threat, risk, or confinement of alternatives
- The fear of loss of further freedoms can motivate reestablishing the threatened freedom

Raising privacy awareness within context aware services seems to contradict the service provider's interests.

Towards a Research Approach

Goal: Assisting average individual users to identify and assess pitfalls and risks related to the disclosure of personal information in context-aware services.

Research Question: How to integrate privacy awareness on an application specific level from an organisational perspective?

Design Science Paradigm in Information Systems Research: Search for artefacts to proactively address relevant problems.

Expanded Privacy Awareness

H1: To overcome the privacy paradox, raising privacy awareness on an application specific level should be closely connected with raising knowledge about methods and tools essential to satisfy needs with regard to the protection of privacy in a meaningful way.

- Awareness of problems + Awareness of possible solutions
- Users have to be provided with means to satisfy raised privacy needs, otherwise they will abstain from providing personal information

Resulting Incentives

H2: Raising privacy awareness in connection with providing privacy enhancing technologies on an application level can strengthen the relationship between user and provider of a services.

H3: The combined approach of raising privacy awareness and providing means to react will result in a higher disclosure of personal data and retention rate.

Concluding Remarks & Outlook

Contribution of this article according to Hevner's framework:

- Problem Relevance (Guideline 2)
  - Privacy Paradox
  - Creating Privacy Awareness
  - Organisational & technical challenges
- Proposal and design of an Artefact (Guideline 1)
  - Expansion of the meaning of privacy awareness from awareness of problems towards solutions as means to overcome the privacy paradox

Application of the design science framework by Hevner:

- Enhancement / Re-formulation of hypothesis according to the requirements
- Validation of hypotheses

mobile business

Thank you for your attention!

andre.deuker@m-chair.net