Taking Responsibility for Online Self-disclosure

The thin line between a company’s user orientation and user surveillance

Christine Bauer

Vienna, 22 September 2016

Self-disclosure

Self-disclosure is defined as
what individuals verbally communicate about themselves,
including thoughts, feelings, and experiences.

People disclose information for a variety of purposes:

- establishing legitimacy,
- authentication,
- trust,
- providing personalized services,…

Online self-disclosure

is of particular interest in human-computer interaction

e.g.,

- personalized recommender systems
- “one click” purchasing
- e-recruitment

However, not all users are willing to disclose personal information.

Major barrier: privacy concern

Role of company in this context (1/2)

Is it morally okay to exploit users' personal information for their own profit?

Or do companies have the responsibility to remunerate users whose personal information they exploit?

Do companies have the responsibility to protect users from self-disclosing too much?

Role of company in this context (2/2)

There are two sides of the same coin

- Companies have to respect the users' desire for privacy and cannot collect and exploit at all their PI for companies' profit
- If users give away their PI freely (e.g., on online social networks), why not use it; those that do not want to provide their personal information should not use the offered service

Total surveillance and full privacy are the two extreme poles.

Hybrid forms are possible and currently reality.

Strategies

Privacy by design

Situationalization

Privacy seal

Transparency on personal information use

Service duality

Strategies (1/3)

Privacy by design

- value-sensitive design
- an approach to systems engineering that takes privacy into account throughout the entire engineering process
- critiqued for leaving open questions in how to apply it when engineering systems

Situationalization

- using information characterizing the present situation based entirely on non-personal aspects (e.g., physical context)
- examples are location, time, atmospherics, or the social environment
- eliminates the need for person-related data
  → does not require users to self-disclose

Strategies (2/3)

Privacy seal

- privacy indicator, statement, or seal to informs users about the privacy efforts of company
- may be used in addition to privacy by design or a situationalization
- Privacy seals have been reported as having only moderate effects on OSD

Transparency on personal information use

- Collecting and leveraging users' personal information and clearly informing them in advance about data use
- current practice: long data policy statements that are little informative and/or hide the relevant statements on personal information processing → company taking the responsibility role seriously will put effort in making policy transparent and understandable

Strategies (3/3)

Service duality

- offering two systems/services with different functionality: users with different attitudes towards OSD are served with different services
- implies additional costs; but balanced by service pricing: Some people pay for maintaining their privacy; others pay for getting access to additional features in exchange for OSD

Future work and respective methods

Systematic elicitation of strategies

- Systematic literature review?

Systematic evaluation of strategies

- Literature review?
- Expert interviews?

The “how” question

- Expert interviews?

Christine Bauer

E chris.bauer@univie.ac.at
W www.christinebauer.eu

University of Vienna
Oskar-Morgenstern-Platz 1, 1090 Vienna, Austria