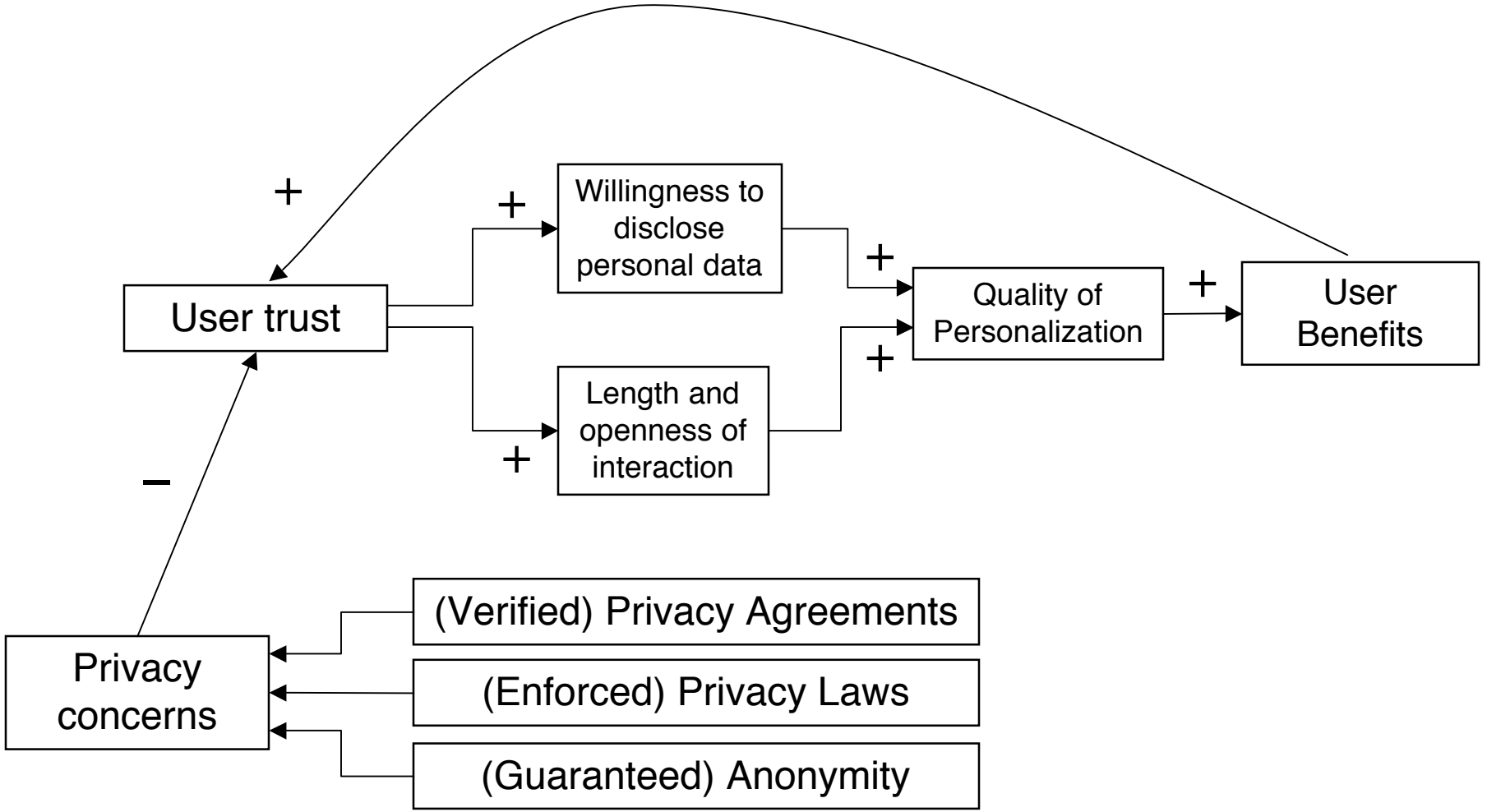
Current Work on Privacy in Personalized Systems

Alfred Kobsa
University of California, Irvine

Privacy and Personalization



Privacy through Pseudonymity in User-Adaptive Systems

Guarantee privacy in user-adaptive systems through pseudonymity whilst fully preserving personalized interaction.

Desired properties (ISO 15-408-2, Pfitzmann & Köhntopp 2001)

- [latently] **unidentifiable**: neither the personalized system nor third parties can determine the identity of pseudonym-ous users
- **linkable for the user-adaptive system***:* the personalized system can link every interaction step of a user, even across sessions (users maintain a persistent identity)
- **unlinkable for third parties***:* third parties cannot link two interaction steps of the same user
- **unobservable for third parties***:* the usage of a personal-ized application by a user should not be recognizable by third parties

Reference model for pseudonymous and secure user modeling

- Permissions server for role based access control
- Mix network for hiding the identities of users and of user modeling servers
- Secure transport
- Certificate directory
- Reference monitor that safeguards the access of user modeling clients to user models located in the **user modeling server**.

Paper in the *ACM Transactions on Internet Technology*, May 2003 (with Jörg Schreck)

2. Impacts of User Privacy Preferences on Personalized Systems

- Meta-review of 30 consumer surveys on privacy preferences
- Studying impacts on personalized systems

Paper at the *CHI 2003 Workshop on Designing Personalized User Experience*, Fort Lauderdale, FL (with Max Teltzrow)

3. Requirements on personalized systems imposed by international privacy laws

Compilation of 27 laws at
http://www.ics.uci.edu/~kobsa/privacy/intlprivlawsurvey.html (w/ X. Chen)