Challenges of Usable Privacy and Security

2022-05-31

KARLSTAD
UNIVERSITY
SWEDEN

Simone Fischer-Hübner

(Recent joint work with Ala Sarah Alaqra, Matthias Beckerle, Jan Eloff, Erik Framner, Bridget Kane, Farzaneh Karegar, Eunice Hammond, Lejla Islami, Thomas Lörunser, Patrick Murmann, John Sören Pettersson, Delphine Reinhardt)

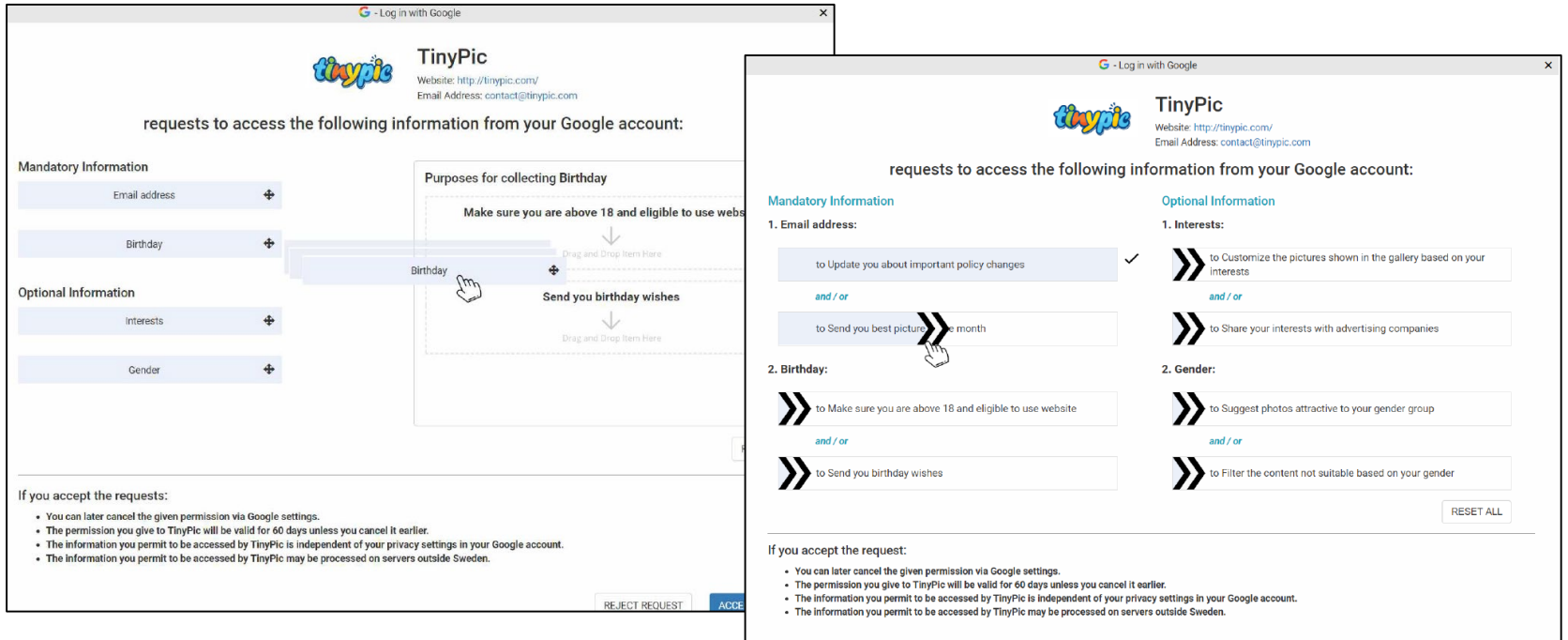
Challenges of Usable PETs:

1. Privacy/Security is usually only a secondary task

Challenges of raising the users' attention for privacy decisions / consent

Example:

Different types of **affirmative (inter-)actions** may affect user attention **to certain parts of policy information**

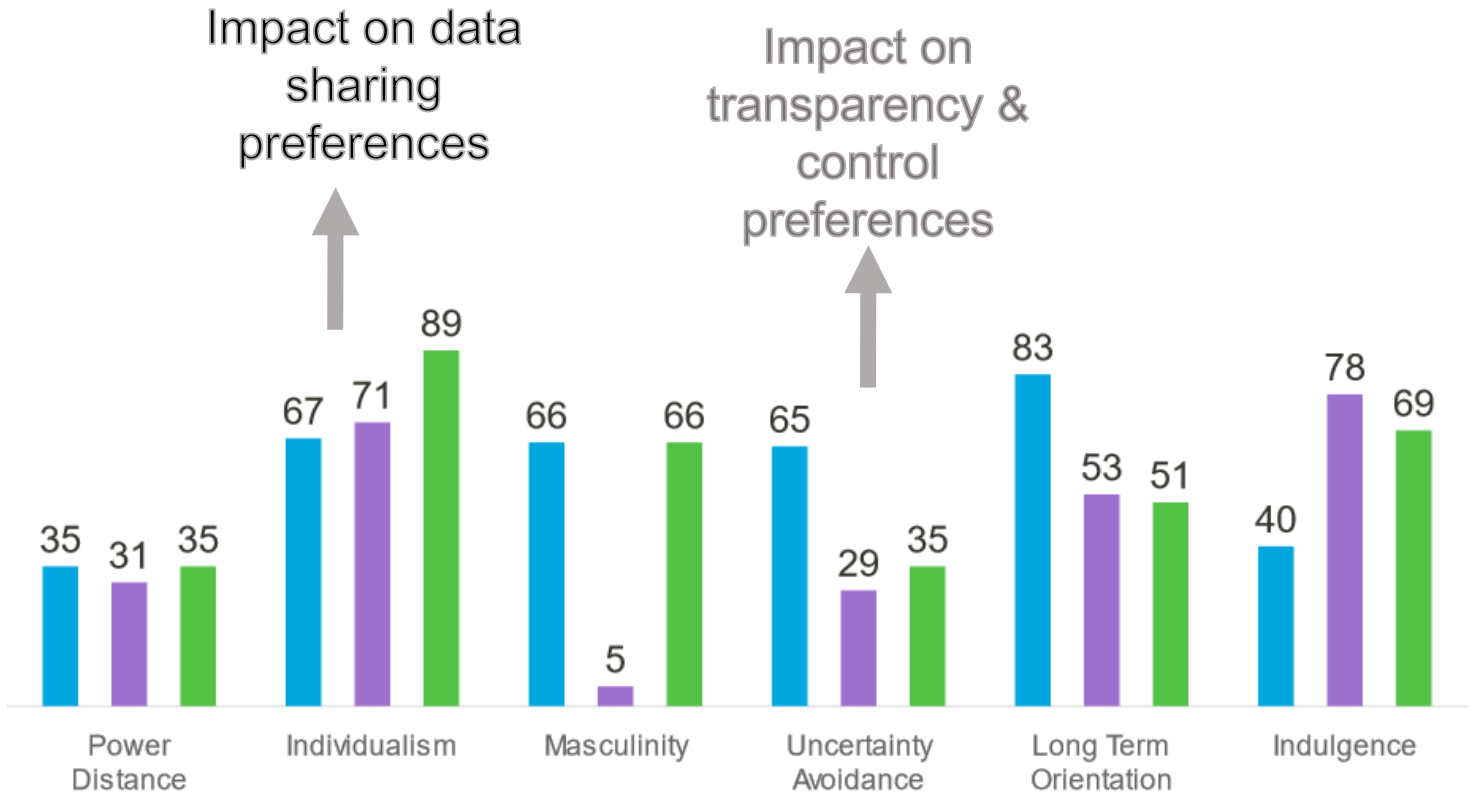


- Petterson, J.S., Fischer-Hübner, S. et al., (2005). *Making PRIME usable.* SOUPS 2005. ACM Digital Library.
- Karegar, F., Pettersson, J. S., & Fischer-Hübner, S. (2020). *The dilemma of user engagement in privacy notices: Effects of interaction modes and habituation on user attention.* ACM Transactions on Privacy and Security (TOPS), 23(1), 1-38.

CREDENTIAL

Challenges of Usable PETs:
2. Cultural Dimensions of Privacy Preferences / Personas

Hofstede Insight – Country Comparision



https://www.hofstede-insights.com/country-comparison/

- Alaqra, A. S., Fischer-Hübner, S., & Framner, E. (2018). *Enhancing privacy controls for patients via a selective authentic electronic health record exchange service: Qualitative study of perspectives by medical professionals and patients*. *Journal of Medical Internet Research (JMIR)*, *20*(12).
- Murmann, P., Beckerle, M. , Fischer-Hübner, S., Reinhardt, D., *Reconciling the What, When and How of Privacy Notifications in Fitness Tracking Scenarios*. Pervasive and Mobile Computing 77 (2021): 101480. Elsevier
- Islami, L., Fischer-Hübner, S., Hammond, E. & Eloff, J. (2021). *Analysing Drivers' Preferences for Privacy Enhancing Car-to-Car Communication Systems*. Springer

Cyber Security for Europe

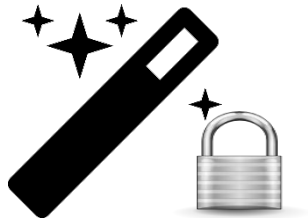
Privacy & Us

South Africa Sweden University Forum

SURPRISE

Challenges of Usable PETs

3. Perceptions of PETs - Finding suitable metaphors & explanations



Challenge: PETs based on ”crypto magic”

- hard to comprehend or trust the privacy functionality
- hard to find real-world analogies as metaphors
- Technical background knowledge may have a negative impact on mental models

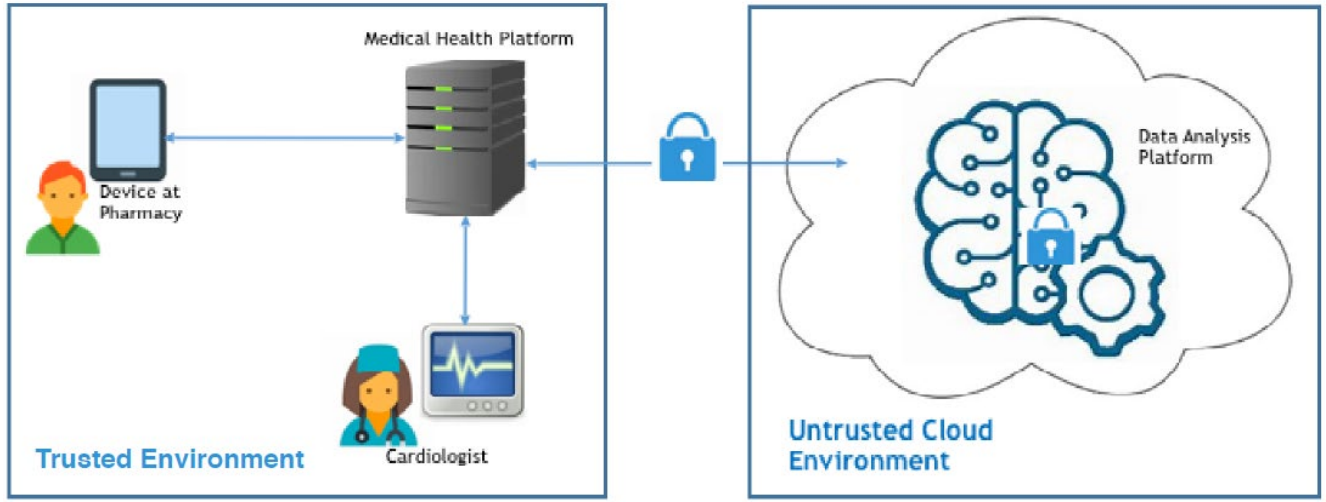
Example: Platform for Privacy-Preserving Data Analytics

Evaluation results:

- **Homomorphic Encryption:**
  Skeptism / Distrust in claims on data analysis of encrypted data

- **Homomorphic Encryption & Differential Privacy:**
  Mental models may be impacted by knowledge about other security tools

- **DP- Misconception triggered by digital-world analogies**
  - Examples
    - Knowledge of encryption - > DP is reversible
    - Knowledge of VPNs -> DP = selective disclusure
    - Knowledge of firewalls -> DP = access control



- Alaqra A.S, Kane B., Fischer-Hübner S. (2021). *Machine Learning Based Analysis of Encrypted Medical Data In The Cloud: A Qualitative Study of Expert Stakeholders' Perspectives*, Journal of Medical Internet Research - JMIR Human Factors 2021;8(3):e21810.
- Karegar, F., Fischer-Hübner, S. (2021). *Vision: A Noisy Picture or a Picker Wheel to Spin? Exploring Suitable Metaphors for Differentially Private Data Analyses*. EuroUSEC Symposium. ACM.
- *Karegar, F., Alaqra, A. Fischer-Hübner, S. (2022). Exploring User-Suitable Metaphors for Differentially Private Data Analyses. Forthcoming.*

CONCUSIONS – ADDRESSING CHALLENGES

- Raising **user attention to (secondary) privacy policy tasks** depends on the information presentation & **modes of interactions**
- **Cultural dimensions** need special considerations for User-Centred Design
- Both real-world & **digital-world analogies** for PETs need to be considered

Thanks !

KARLSTAD
UNIVERSITY
SWEDEN