Privacy-ABCs as a Case for Studying the Adoption of PETs by Users and Service Providers

Ioannis Krontiris, Zinaida Benenson, Anna Girard, Ahmad Sabouri,
Kai Rannenberg, and Peter Schoo.

Motivation

- PETs are not widely adopted in practice
- Technical features are there, but socioeconomical aspects not fully addressed
- Economic costs and benefits of PETs
  - Technology specific
  - Application specific
- We focus on one PET and one application scenario
  - Privacy-ABCs
  - Anonymous Surveys
- We explore factors affection adoption of Privacy-ABCs
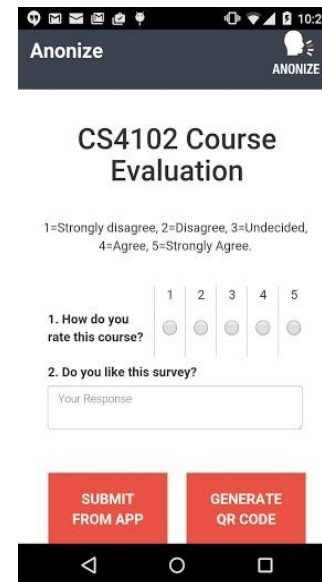 - from the user's side
  - from the service provider's side

Use Case: Anonymous Surveys

Survey responders can speak their minds with the assurance that it's mathematically impossible for anyone to identify them.

Case 1: EU-Project ABC4Trust

Case 2: Anonize Project (Cornell Tech)

Advantages of Privacy-ABCs

- ## Privacy-ABCs are by default untraceable
  IdSPs are not able to track and trace at which sites the user is presenting the information

- ## Privacy-ABCs can be obtained in advance and stored
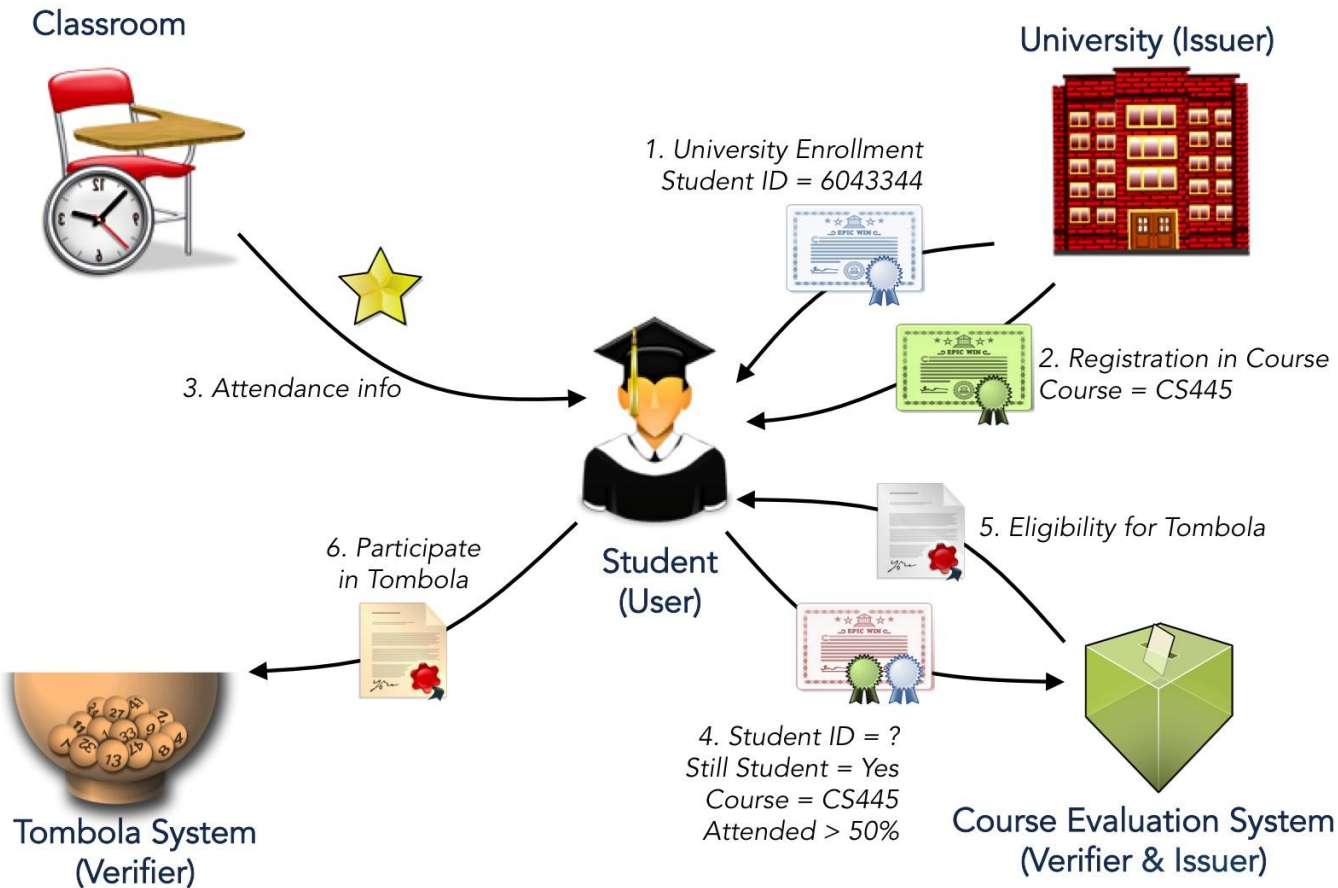 No real-time burden of the IdSP – better scalability

- ## User-binding
  No credential pooling possible – Presentation requires proof of knowledge of a secret key (stored on a secure device like SC)

- ## Unlimited number of pseudonyms supported
  In addition to which, scope-exclusive pseudonyms can be imposed – user can only register one pseudonym per scope (URL).

Patras Pilot of ABC4Trust

Classroom

University (Issuer)

1. University Enrollment
Student ID = 6043344

2. Registration in Course
Course = CS445

3. Attendance info

Student
(User)

5. Eligibility for Tombola

6. Participate
in Tombola

4. Student ID = ?
Still Student = Yes
Course = CS445
Attended > 50%

Tombola System
(Verifier)

Course Evaluation System
(Verifier & Issuer)

Course Evaluation

Patras Pilot User Trial

- Course "Distributed Systems I" (80 students)
- 42 students participated in the pilot with a SC
- From 23. November 2012 – 11. February 2013
- Printed questionnaires distributed to 54 students

Questionnaire:
- 54 students: 23 years old on average (36 male, 18 female)
- 41 respondents used the system,
- 13 did not used the system

Goal of the questionnaire:
- What factors influence user acceptance of Privacy-ABCs?

Technology Acceptance Model (Davis 89)

Classic TAM considers Perceived Usefulness and Perceived Ease of Use as main factors in user acceptance
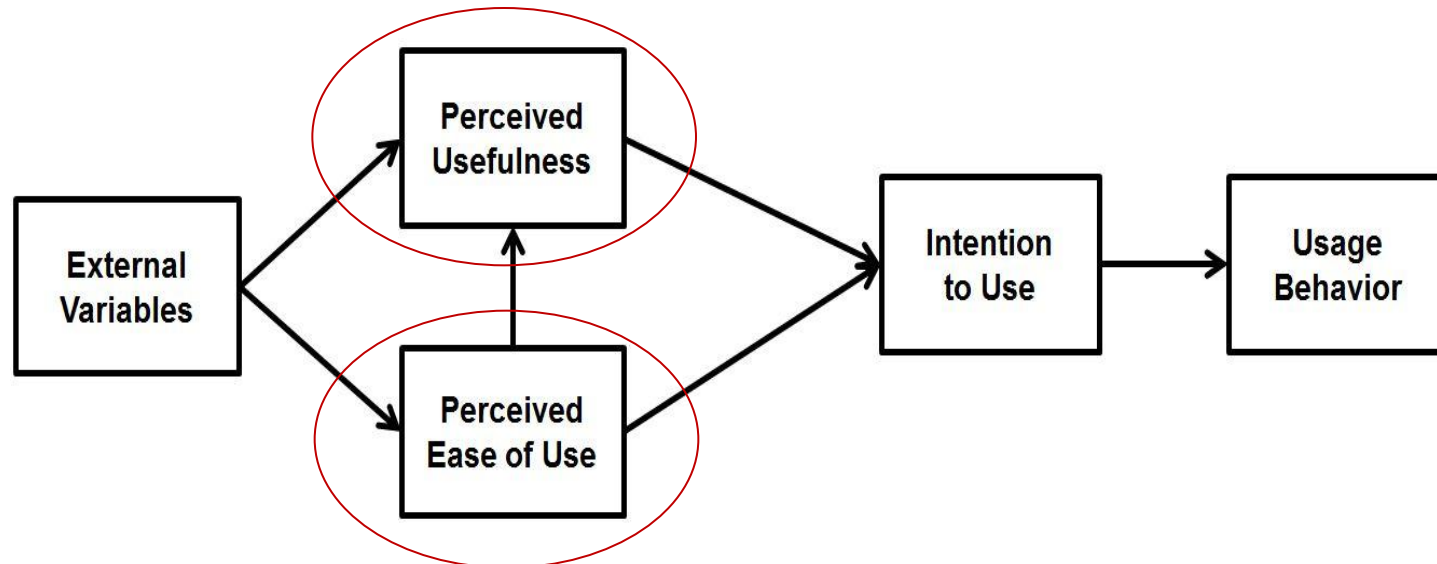
Adaptation of Perceived Usefulness

- PU for the Primary Task (PU1)
  - Degree to which a person believes the system to be useful for the **primary task** (= course evaluation)

- PU for the Secondary Task (PU2)
  - Degree to which a person believes the system to be useful for the **secondary task** (= privacy protection)

- Novel extension to the TAM
  - Specific to security- and privacy-enhancing technologies

TAM + Trust + Risk (Pavlou 03)

Pavlou integrated Trust and Perceived Risk into the TAM, which we also considered in our model.
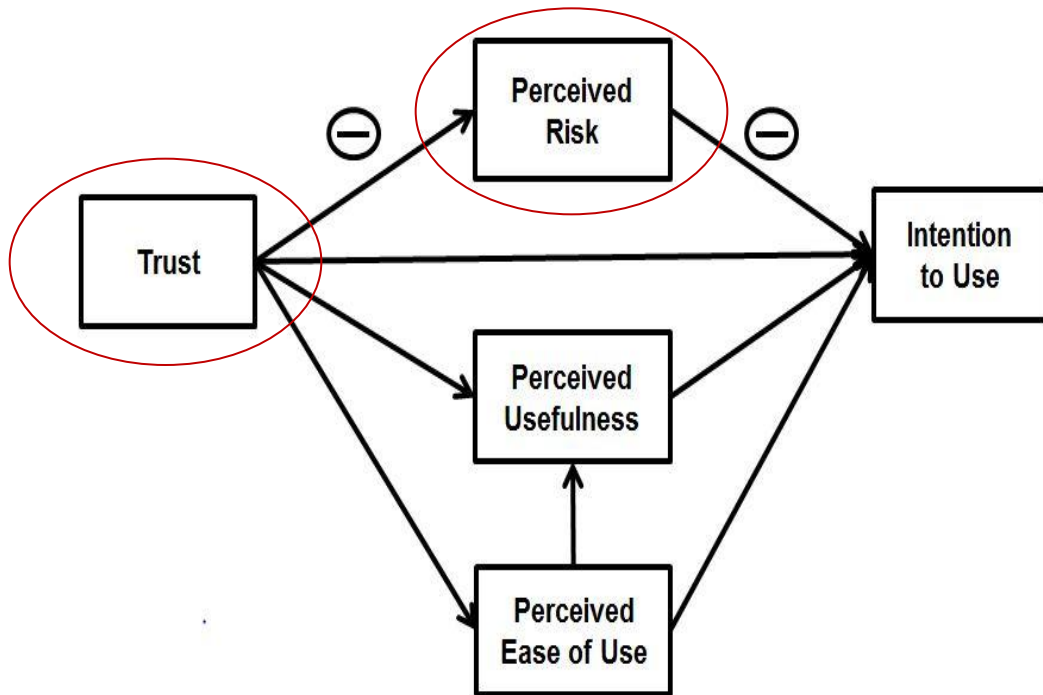
• Trust into the Privacy-ABC technology
• Perceived Risk of usage of Privacy-ABCs

The model so far...
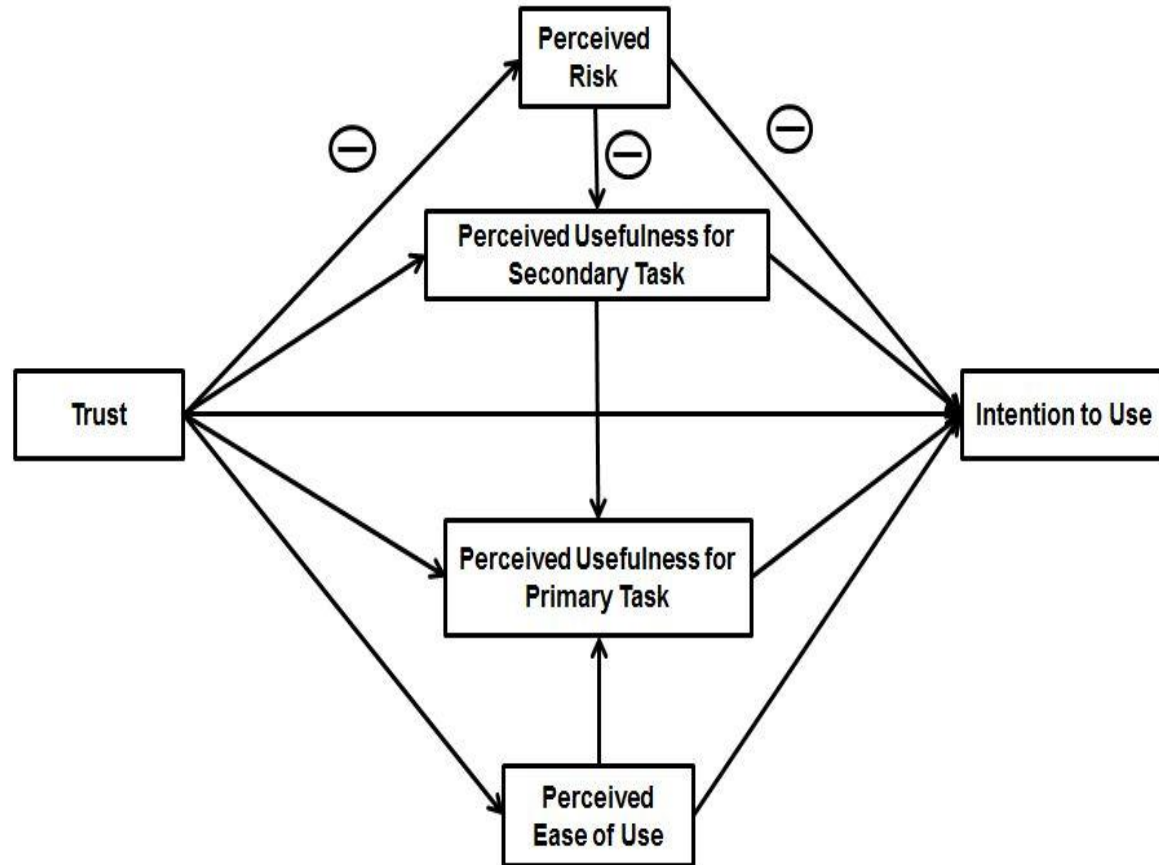
The model so far…
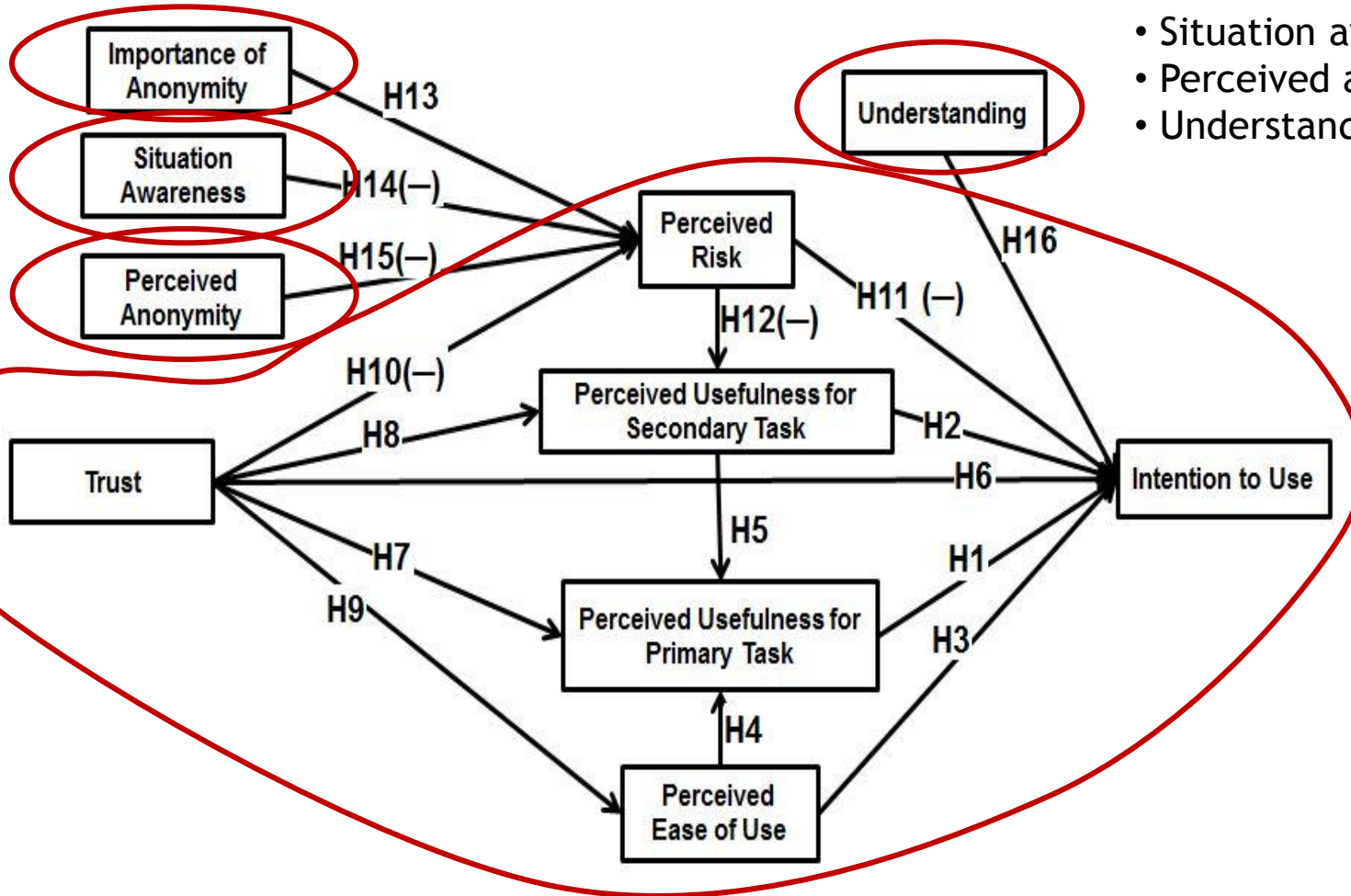
Additional factors:
- Situation awareness
- Perceived anonymity
- Understanding of technology

Conclusions for users' side

- Ease of Use, both kinds of Perceived Usefulness, Trust and Situation Awareness are significantly positively correlated to the intention to use Privacy-ABCs

- Perceived Risk is significantly negatively correlated

- Perceived Usefulness for Primary Task is the most important one for user acceptance

- no correlation between the Understanding of Privacy-ABCs and the intention to use them

- Analytical details are presented in the following paper:

Z. Benenson, A. Girard, I. Krontiris, "User acceptance factors for anonymous credentials: An empirical investigation", In Workshop on the Economics of Information Security (WEIS), 22-23 June 2015.

Cost-Benefit Trade-Offs

Usability issues

- Mental effort
  - Interaction with the system
- Physical effort
  - E.g. handling smartcard, etc.
- Learnability effort
- Memorability effort
  - Remembering how to interact with it
- Low helpfulness
  - Help information provided
- Error recovery effort
- Worries about smartcard loss
- Uneasiness about data on smartcard

Perceived usefulness

- For primary task
- For secondary task

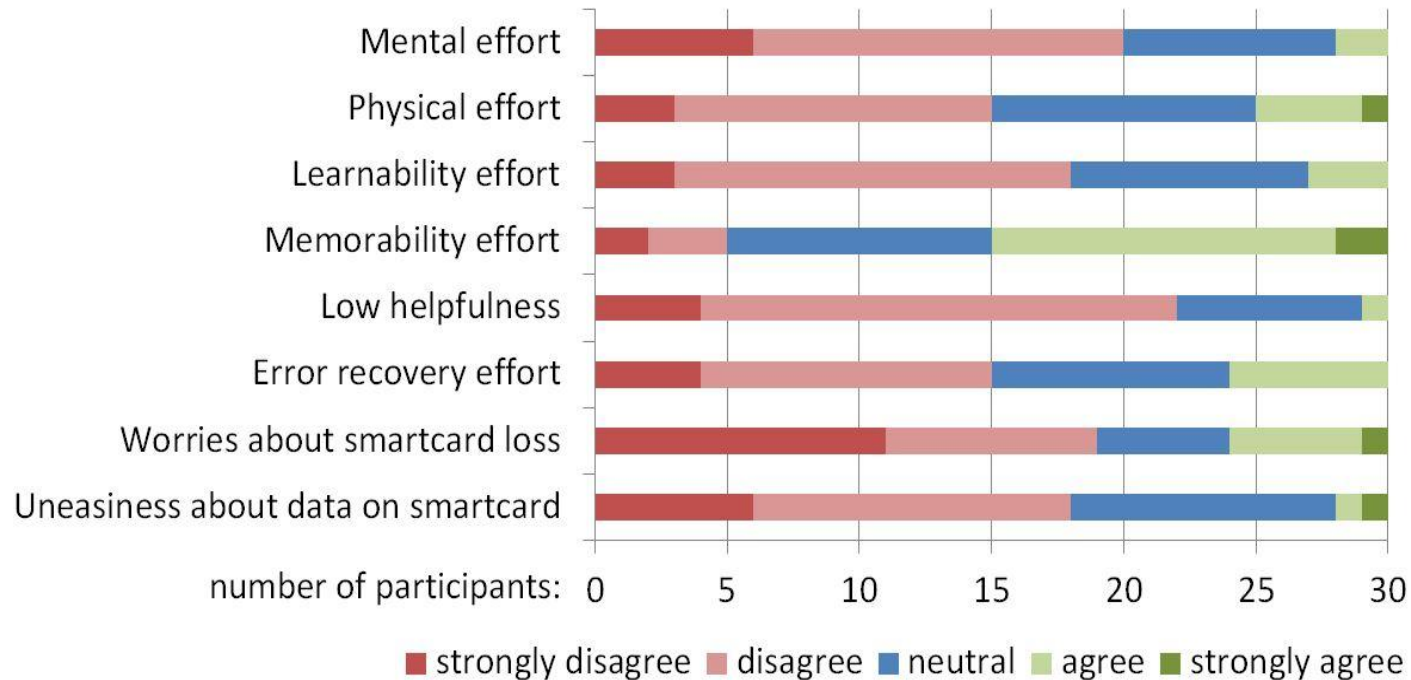# Usability Costs of Privacy-ABCs

Adoption of PETs by Service Providers

- Technology
  - Compatibility with existing protocols and standards
  - Complexity to understand and use
  - Trialability and Observability
- Organization
  - Top management support
  - Business model dependency on user data collection
- External Pressure
  - Regulatory pressure
  - Social pressure
  - Extend of adoption among competitors
  - Standardization
- Environment
  - Established infrastructure readiness

[A. Sabouri, "Understanding the Determinants of Privacy-ABC Technologies Adoption by Service Providers", to appear in IFIP I3E 2015]

Cost-Benefit Trade-Offs

- Data usability loss
  - Business models currently based on personal data
- Social loss
  - Uncertainty created to users
- Integration and deployment costs
  - Lack of engineering practices for PETs
  - Different standards and regulations
- Educational costs
  - Educate the users how to use it

- Reduced risk of data breaches and misuse
  - Efficient protection of personal data
- Reduced reputation loss
  - Regulation mandates disclose of privacy failures
- Better protection of trade secrets
  - Unlinkability property

Recommendations

Users

- still missing more and broader field trials to explore the socioeconomic factors of privacy technologies.
- we should investigate not only adopters, but also non-adopters of PETs in order to better understand the acceptance factors.

Service provider

reliable data to inform the analysis:

- there is a need of reliable estimates of the potential loss from a privacy incident.
- data on the reputation impact of privacy breach notifications or on the revenue loss of firms due to privacy concerns.