

ACCEPT

Acceptable Use of Privacy-Enhancing Technologies

Dr Katharina Burger (PI), The University of Bristol

Dr Claudia Peersman (Co-I), The University of Bristol

Dr Baraa Zieni (Research Associate), The University of Bristol

November 2021



PETs are a “*coherent system of ICT measures that protects privacy [. . .] by **eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system***”
(Borking and Raab, 2001 p.1)



(Cf. Asrow and Samonas, 2021)

bristol.ac.uk

Context: Privacy risks

- Collect, track, monitor “surveillance”
- Aggregate, Analyse “process”
- Distribute, communicate “networks and platforms”

Top use cases of PETs

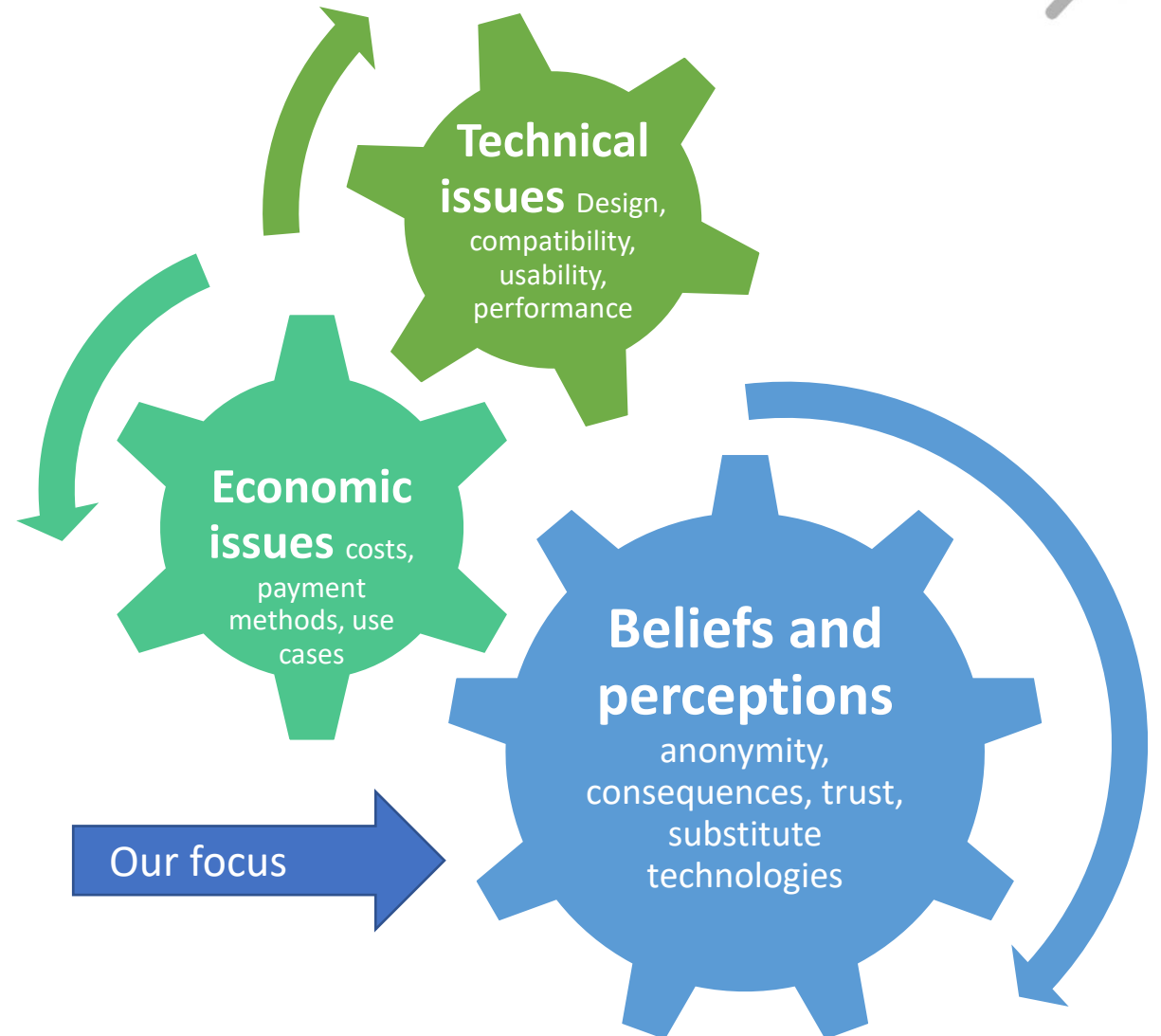
- Financial transactions
- Healthcare services
- Facilitating data transfer between multiple parties including intermediaries



Socio-technical systems!!!!

The challenge: people's behaviour

- Successful implementation and adoption of PETs **requires a profound understanding of the perceptions and behaviours of actual and possible users** (at organizational and end-user levels)
- ACCEPT aims to investigate **consumer perspectives on the use and sharing of PETs-related data** by various types of 'legitimate' organisations
 - Started 09/2021
 - Currently in research design phase



Getting to grips with research in this area

- 39 papers retained (>600 scanned, 2015 to date)



Private Machine Learning	Cryptography	Privacy Policies
Data Privacy I	Multiparty Private Machine Learning I	Privacy Preferences
Data Privacy II	Multiparty Private Machine Learning II	Privacy Behaviors
Privacy Attacks	Applied Cryptography I	Privacy Awareness
Web Tracking	Applied Cryptography II	Internet of Things Privacy
Censorship and Certificates	Cryptography and Cryptocurrencies	Mobile Privacy
Website Fingerprinting	Secure Multiparty Computation	DNS and Privacy



Sector-specific papers: Smart homes, Agriculture, Healthcare (apps), Freight/Transport/Security

Specific demographic groups

Specific contextual/situational factors

Awareness, perception and motivation

- Privacy concerns and privacy behaviours
- Usability – privacy trade-off
- Awareness, understanding and consent:
 - settings, notification preferences, recording data storage
- Understanding security advice
- Awareness of privacy-enhancing tool, interest in preventing threats, misconceptions

Linguistic understanding/terminology and information visualisation, incl. user design (consent dialogues)

The role of AI/machine learning in understanding user preferences

Some research questions in the sample of papers

- **‘Second-order’ categories of users**
 - To what extent are **incidental users** concerned about the privacy risks of smart-home devices? In what capacities, contexts, and situations are people **exposed to other people’s smart-home devices**?
- **Stated preferences vs actual behaviour studies**
 - What (perceived) benefits and harms do they **experience**?
- **Change in preferences/unstable preferences**
 - what circumstances may change original decisions
- **Communication suitable for specific groups, .e.g. young women**
 - how well do developers inform menstruapp users about their privacy practices within their policies and privacy communications?
- **Information visualisation, language use, etc**
 - Are users able to understand the purpose of the privacy visualizations and the data flows depicted by the visualizations at-first-glance?

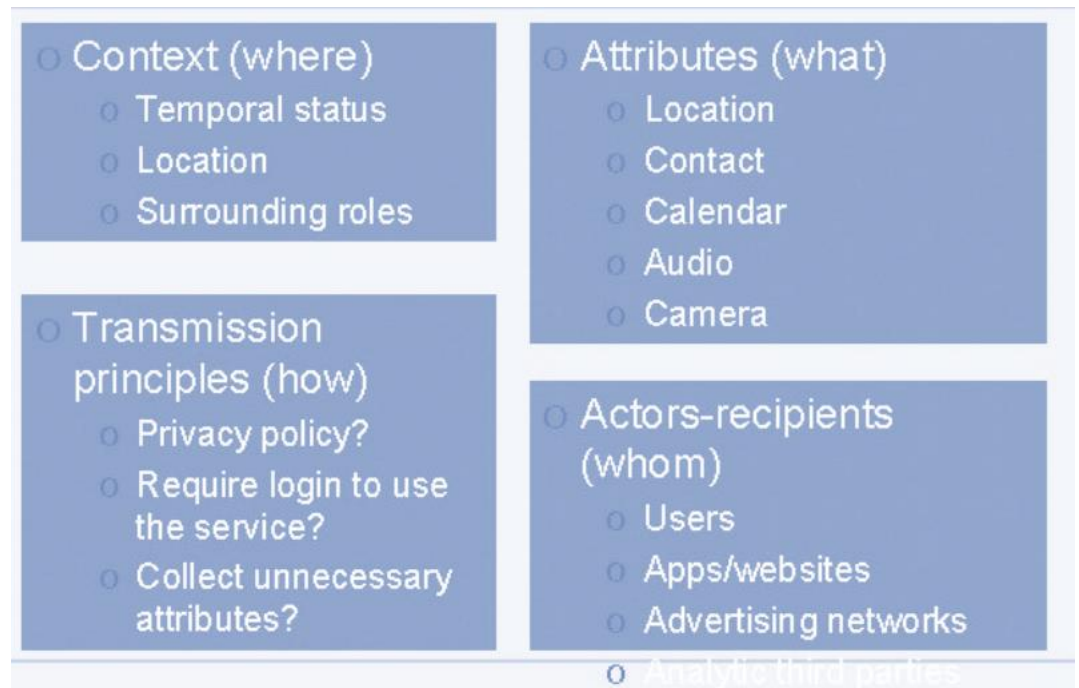


Tackling these questions: examples of theoretical frameworks applied in the study of PETs

Some of the theories used:

- **Contextual Integrity Theory** (Nissenbaum, 2004).
- Privacy Management (CPM) theory (Petronio, 2002).
- Components of Protection Motivation Theory (Albayram et al., 2017).

“Contextual integrity is preserved *when* information **flows** conform to **legitimate contextual informational norms**”
(Nissenbaum, 2021)



Example of operationalisation of CIT

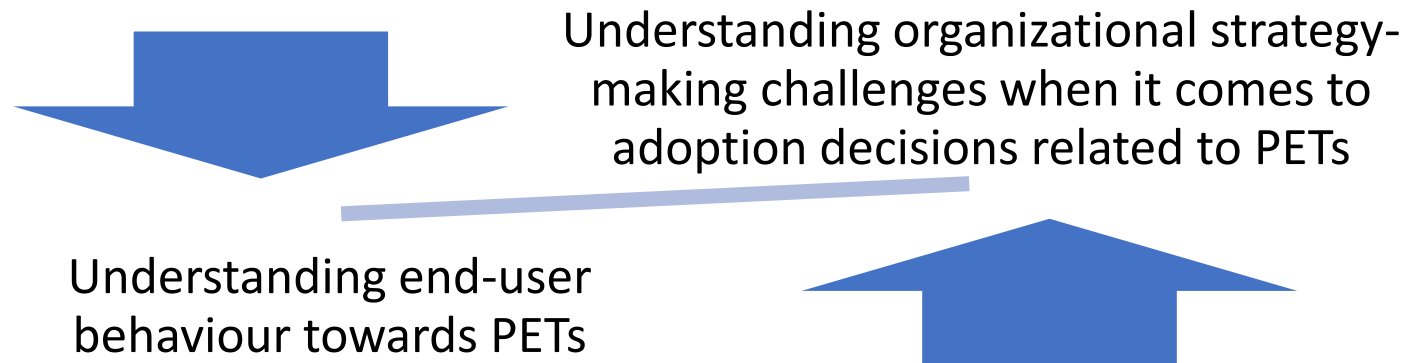
So what? Implications for ACCEPT



Privacy-sensitive
Business Models:
Barriers of
Organizational
Adoption of Privacy-
Enhancing
Technologies

Willingness to pay
e.g. for smart home
privacy?

Implications for ACCEPT: co-creating the behavioural studies



We have the (human) resources – you have the real-world experience/challenges:

How can we make this research most relevant to you?

We are looking for organisations that would like us to

- Facilitate a workshop/conduct expert interviews in their organization to **elicit/co-design their strategically-relevant questions relating to PETs adoption**
- Help us **identify a possible user group** to conduct the research (survey, interviews, experiment, focus group) on **to answer their strategic questions**



**COULD
YOU BE
THE
ONE?**



If you are interested in the research:

Please contact the PI:

Dr Katharina Burger

Senior Lecturer in Management

The University of Bristol

katharina.burger@bristol.ac.uk



To learn more about REPHRAIN, our future plans and how to get involved:

 www.rephrain.ac.uk

 @REPHRAIN1

 rephrain-centre@bristol.ac.uk

We would love to hear from you. Thank you!