



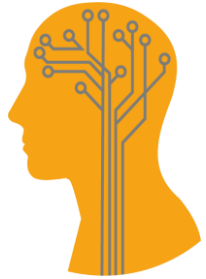
User Perceptions of AI, Privacy, the GDPR and PETs

‘Online Services: Improving consumer usability and trust’

Dr. Sebastian Pape | TDL Roundtable

Agenda

› Perception of AI



› Perception of Privacy



› Perception of GDPR



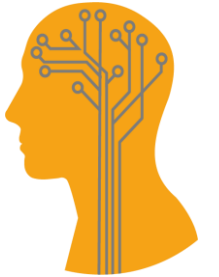
› Perception of PETs



Perception of AI

- › **No clear understanding of AI**
 - › “Everything is called AI”
- › **Mystery black box with output**

- › **Explainable AI**
 - › Not only provides a ‘solution’
 - › But also an explanation how it was derived



Perception of Privacy

› Privacy Concerns

- › Might prevent users from adopting to a service

› Users

- › Don't want to be bothered
- › Often don't understand the (long-term) effects of tracking / data collection
 - › "I've got nothing to hide"



Perception of GDPR

- › **Annoying forms everywhere**

- › Doctor
- › Garage
- › Landlord
- › ...

- › **Cookie „consent management“ on websites**

- › Bother users to get consent
- › Dark patterns



Perception of PETs (Tor)

- › “Increased latency makes the experience painful at times”
- › “It can’t be used on all websites; therefore it is of limited use to me”
- › “For the same reason I don’t hang out in brothels, using Tor makes you look like a criminal”
- › “[. . .] having a cop boot at my door because of Tor”

- › “It is a key component to maintaining one’s privacy when browsing on the Internet.”
- › “Tor protects privacy while on the web and is easy to use.”



Harborth, D.; Pape, S. and Rannenber, K.: **Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym**. In Proceedings on Privacy Enhancing Technologies (PoPETs), 2020 (2): 111-128, 2020.

Challenges for implementing PETs I

- › A good PET
 - › Is barely noticeable by the user
- › How can users then reward PETs?
- › User needs to understand how the PET works
- › Challenge: How to explain to the user?
 - › Homomorphic encryption
 - › Multi Party Computation
 - › Privacy Preserving Machine Learning
 - › k-anonymity
 - › (Distributed) Differential Privacy
 - › Federated Learning
- › Users don't want to know all details



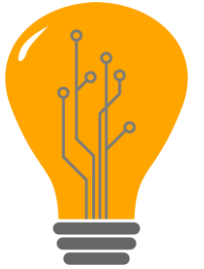
Challenges for implementing PETs II

- › How can users get assurance / trust a PET is in place?
- › For AI we had explainability
- › For PETs?
 - › Provide list of integrated PETs?
 - › How does the user know
 - › A suitable PET was chosen?
 - › It was applied / implemented correctly?
- › How do we differ between 'real PETs' and 'PETwashing'?
 - › How about a 'privacy label'?
 - › Creates overhead for auditing
 - › Time and resources are better invested in improving the product



A first step

- › Companies / Technology providers need to learn:
- › A privacy-friendly service (including PETs) is not a contradiction to functionality or business models.
- › Fines from the GDPR foster this
- › **Clive Humby (2006):** *“Data is the new oil. It’s valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc to create a valuable entity that drives profitable activity; so must data be broken down, analyzed for it to have value.”*
- › But like oil (pollution), data can also be a liability.



AUTOPSY

Automotive Data-Tainting for Privacy Assurance System



France

> Paris



Germany

> Frankfurt



> München



1st July 2021 – 30th June 2024



Research Project partly funded by BMBF



To create better understanding of **Data flows** in **Automotive environments**



To create **Privacy-Aware System Model** for an **Automotive Use-Case** in specific **technical design**

Thanks for your Attention

Any Questions?



PD Dr. Sebastian Pape
Security & Privacy Manager

Continental Automotive Technologies GmbH
Security & Privacy Competence Center – SCC
Guerickestraße 7
60488 Frankfurt am Main, Germany

Phone: +49 (69) 7603-72199
E-Mail: sebastian.pape@continental.com

