

A Loving Home for PETs? Surveillance States and Big Tech Co-Opting Privacy-Enhancing Technologies

Felix Bieker & Marit Hansen

It has often been stated that the adoption of Privacy-Enhancing Technologies (PETs) has been slow and cumbersome in practice [see already London Economics 2010]. While there is no shortage of academic publications on PETs focussed on ideas, concepts and projects [Hansen 2008; Hansen 2013, Hansen et al 2015] we rarely see the adoption of PETs in real-life applications. For public sector projects, a factor may well be that the possibilities for surveillance are a feature, rather than a bug. State actors, including the European Union (EU) and its Member States, have consistently been advancing their surveillance apparatus. They can simply legalize invasive practice by passing corresponding legislation and thus might have few incentives to implement real privacy-enhancing standards, infrastructures and technologies. With the current rush on so-called Artificial Intelligence (AI)

At the same time, unlikely contenders for PET implementation appear to have entered the stage: Big Tech companies, such as Uber and Amazon are using PETs in their processes [Data & Society 2025]. However, their practices raise serious concerns with regard to privacy and data protection. Uber, for instance, uses differential privacy to surveil employees through generalized profiles and performance metrics. Amazon, on the other hand, uses synthetic data to predict worker behaviour. This enables it to bypass labour and data protection regulations, while enabling AI based decision-making that may degrade working conditions.

In this workshop, we will give participants an overview over PETs, their possible uses and current developments in PET adoption. We will introduce value-based design approaches and draw attention to potential adverse effects possibly associated with the application of certain PET approaches that, for instance, render data subject rights ineffective [Veale/Binns/Ausloos 2018] or that affect other fundamental rights, data protection. Further, we introduce participants to the EU legal framework that applies in the example cases, especially the AI Act and the Platform Work Directive.

We will facilitate a discussion on the ramifications of the implementation of PETs for surveillance of workers and how such abuses of PETs can be avoided. In the discussion we want to give a platform for early-stage as well as experienced researchers for discussing value-based design of technologies, risks for privacy and data protection that may be caused by uses of PETs. Together we want to explore the potentials of adopting PETs to advance privacy and data protection and how to avoid misuses and co-opting of these technologies.

References:

- Data & Society, The “Privacy” Trap: How “Privacy-Preserving AI Techniques” Mask the New Worker Surveillance and Datafication, Policy Brief 2025, <https://datasociety.net/library/the-privacy-trap/>
- Marit Hansen, (2008): Marrying Transparency Tools with User-Controlled Identity Management. In: The Future of Identity in the Information Society: Proc. Third IFIP WG 9.2, 9.6/11.6, 11.7/FIDIS International Summer School on The Future of Identity in the Information Society IFIP AICT 262, pp. 199-220.
- Marit Hansen, (2013): Data Protection by Default in Identity-Related Applications. In: Proc. IDMAN 2013, IFIP AICT 396, pp. 4-17.
- Marit Hansen et al. (2015). Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies: Methodology, Pilot Assessment, and Continuity Plan. Heraklion: European Union Agency for Network and Information Security (ENISA).
- London Economics (2010). Study on the economic benefits of privacy-enhancing technologies (PETs). Final Report to the European Commission DG Justice, Freedom and Security
- Michael Veale, Reuben Binns, Jef Ausloos (2018): When data protection by design and data subject rights clash, International Data Privacy Law, Volume 8, Issue 2, pp. 105-123, <https://doi.org/10.1093/idpl/ipy002>.