




People-Centred AI  
UNIVERSITY OF SURREY

 Oblivious

CALYPSO AI

 SYNTHESIZED

expeditions

# Enabling AI Innovation Privacy and Security Issues

## Breakfast Workshop

26th of April 2023 / 08:30-11:00AM  
National Liberal Club - London, UK

Surrey Institute for People-Centred Artificial Intelligence, Synthesized, Calypso AI, and Oblivious AI will co-host a working breakfast on the privacy and security issues related to the use of AI, particularly in the light of the recent advances in large language models (LLMs).

The Workshop, held in person, will bring together industry, academia, and policy representatives to discuss the key security and privacy issues associated with the use of advanced machine learning, particularly when computing on sensitive data-in-use.

08:30-09:00	Registration	
09:00-09:10	Organisers' welcome	
09:10-09:30	Participant introduction session	
09:30-10:30	Panel Session 1: AI Security	<i>Chair: Mikolaj Firlej - General Partner at Expeditions Fund</i>
10:30-11:00	Panel Session 2: AI Privacy	<i>Chair: Andrew Rogoyski - Director of Innovation at University of Surrey</i>

The rapid pace of evolution in the AI landscape has organisations racing to be able to deploy measures in order to ensure the security of systems that are developed in-house or adopted from third-parties.

In order to keep pace with this rapidly shifting landscape it is important to implement frameworks and solutions that will enable organisations to avoid bottlenecks while staying compliant to rules and regulations and maintaining the safety of their data and their customers' data.

Themes and questions like the following will be discussed:

- Evolution of LLMs and impact on organisational safety/privacy
- How is AI testing different from traditional testing
- Bridging the AI gap from development to adoption
- How to detect attacks on AI systems
- Rules and regulations around AI safety/privacy
- Who is responsible for AI decisions that go wrong

# Enabling AI Innovation

Dress: smart casual

Wednesday 26th of April

Location: National Liberal Club, Lady Violet Room



People-Centred AI  
UNIVERSITY OF SURREY

The new People Centred AI Institute at the University of Surrey works in partnership with industry, the public sector, government and national AI organisations to deliver a step-change in AI research, training and innovation to deliver the knowledge and skills required to ensure UK leadership of an inclusive and responsible AI-driven economy.

In collaboration with:

expeditions

Expeditions Fund is a long-term and patient venture capital fund investing in early-stage technology companies globally led by mission-driven founders.

 Oblivious

Confidential computing company bringing eyes-off data science. Data governance, collaboration and ML with privacy guarantees.

CALYPSOAI

The leading company in automated AI digital trust software. From AI robustness and security to LLM privacy and DLP.

 SYNTHESIZED

The first API-driven synthetic data generation company on a mission to make the creation and access of high-quality data fast and easy.



 Oblivious

 SYNTHESIZED

CALYPSOAI

expeditions