Department for Science, Innovation & Technology

Republic of Estonia
Ministry of Economic Affairs
and Communications

OECD
BETTER POLICIES FOR BETTER LIVES

United Kingdom - Estonia - OECD Expert Workshop on Privacy Enhancing Technologies and Artificial Intelligence

13 May 2024

Business Events Centre
3-8 Whitehall Place
London, United Kingdom, SW1A 2HH
Zoom: https://meetoecd1.zoom.us/j/96861783008?pwd=ZFB5MkRMVXVTYWs4elN5c0d2bnNNQT09

Final Agenda (rev. 1)

PETs refer to a range of digital technologies and techniques that enable the collection, processing, analysis, and sharing of information while safeguarding data confidentiality and privacy. Currently, there is strong interest in a group of emerging PETs that offer new opportunities in this area. Although many emerging PETs are still in their early stages of development, they hold immense potential to advance privacy-by-design principles and foster trust in data sharing and re-use across organisations and sectors such as health and finance. As such, they play a pivotal role in paving the way for innovative data economy models, including in artificial intelligence (AI).

For example, data obfuscation tools such as synthetic data combined with differential privacy can be used to generate insights or AI models without exposing sensitive or confidential data. In financial services, for instance, they can be applied to financial datasets for fraud detection and credit scoring without exposing the data of specific transactions or clients. And in health care, researchers with the help of AI algorithms can use these tools for disease prediction, drug discovery, and health policy analysis without accessing actual patient records, thus preserving patient privacy.

However, the technical complexity and rapid evolution of PETs present significant challenges not only for policymakers and regulators but also for organisations seeking to implement PETs into their existing business processes and data governance frameworks. This challenge is further exacerbated by the fact that the application of many PETs is confined to specific use cases, which remain largely unknown to prospective users. This raises questions about possible case-specific challenges that need to be addressed as policymakers and regulators seek to achieve wider, more effective, and appropriate adoption of PETs, in line with their regulatory and policy frameworks.

Objectives

This expert workshop aims to help advance policy discussions on PETs by:

- **Highlighting the potential of PETs** for enabling data sharing and the next-generation data economy model with a focus on established and emerging AI-related use cases in the public and private sector, including health and finance;
- **Exploring how governments and regulators can best incentivise innovation in and with PETs,** including in terms of PET adoption;
- **Discussing how to measure and compare the effectiveness and impact of PETs,** including factors to be considered when assessing their choice for a given use case.
- **Fostering an international community of PET experts** to allow for coordinated discussions on the policy and regulatory aspects related to PETs.

By focusing on common use cases of PETs rather than the technologies themselves, this workshop adopts a perspective that is not biased towards a specific type of PET. This approach enables participants to effectively capture the essence of how PETs are employed across various sectors and to more easily adapt lessons learned to sectors beyond those discussed at the workshop. The approach will also help better guide discussions on how governments and regulators can more strategically integrate PETs into their policy and regulatory frameworks for better innovation in and with PETs. It will also help organisations better assess their specific needs for PETs in alignment with their business objectives. In so doing, this workshop will contribute to helping governments and organisations future-proof their data governance and privacy strategies with the help of PETs in the face of evolving technologies and changing regulatory landscapes. **Its discussions will inform the development of an OECD paper on PETs and AI, which will be based on the preliminary content of the background note of the expert workshop.**

Workshop structure and conduct

The following topics will be discussed in dedicated sessions after which a concluding session will address the policy and regulatory implications:

1. Training AI models and verifying their performance without exposing sensitive data;
2. Processing sensitive or confidential data securely within less trustworthy digital environments;
3. Benchmarking the effectiveness of PETs across use cases.

This invitation-only workshop (with no press attendance) is governed by the **Chatham House Rule** to encourage openness and the sharing of information. Under this rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

Following the conclusion of the workshop, in-person participants will be invited to join the informal gathering at the Admiralty (Trafalgar Square, 66 Trafalgar Sq, St. James's, London), at participants' own expense.

<table>
<tr><th colspan="2"><b><i>Agenda</i></b>

<i>Welcome coffee and pastries will be served from 08:30-09:30</i></th></tr>
<tr><td><b>09:30 – 10:00</b></td><td><b>Opening and welcome remarks</b>
• <b>Ms. Felicity Burch,</b> Director, Responsible Tech Adoption Unit, Department for Science, Innovation & Technology, United Kingdom
• <b>Dr. Ott Velsberg,</b> Government Chief Data Officer, Ministry of Economic Affairs and Communications, Estonia
• <b>Ms. Audrey Plonk,</b> OECD Deputy Director of Science, Technology and Innovation</td></tr>
<tr><td><b>10:00 – 10:45</b></td><td><b>Keynote address</b>
• <b>Mr. Marc Rotenberg</b>, President and founder, Center for AI and Digital Policy, United States
<b>Q&A</b> (15 min)</td></tr>
<tr><td><b>10:45 – 11:00</b></td><td><b>Coffee break</b></td></tr>
</table>

11:00 – 12:30	**Session 1: Training AI models and verifying their performance without exposing sensitive or confidential data** This session will explore the use of PETs to facilitate data analysis and the training of AI models. It will cover the use of PETs for input privacy, including data obfuscation tools such as synthetic data as well as tools for decentralised or federated analytics including multi-party computation (MPC). The session will showcase the extent to which these approaches enable the extraction of insights and the development of AI models without the need to access, reveal or centralise sensitive raw data. Use cases to be discussed could include the use of PETs for: • Financial fraud detection and credit scoring without exposing or centralising specific transaction or client data; • Pandemic and disease prediction, drug discovery, and health policy analysis, all without directly accessing actual patient records. Possible questions for discussions: • How can PETs help approach the trade-off between data utility and privacy for AI model training in e.g. finance and healthcare? • What are strengths and challenges in using synthetic data for reliable AI model training compared to other approaches such as federated learning and MPC or encryption in use? • How can model and data quality be assessed and assured, when the underlying data remains inaccessible? **Moderation: Dr. Mark Durkee**, Head of Data & Technology, Responsible Tech Adoption Unit, United Kingdom Department for Science, Innovation & Technology Case study presentations (~7 min each): • **Mr. Roy Cohen**, Head of Big Data, Ministry of Health, Israel • **Mr. Maxime Agostini**, Co-founder and CEO, Sarus Technologies, France • **Mr. Manuel Capel**, Director Business Development, Inpher, Switzerland Lead discussants (~5 min each): • **Ms. Clara Clark Nevola**, Group Manager for AI Compliance, Information Commissioner's Office, United Kingdom • **Mr. Nigel Smart**, Professor - Computer Security and Industrial Cryptography (COSIC), KU Leuven, Belgium • **Mr. Simson Garfinkel**, Visiting Lecturer on Computer Science, Harvard University, United States • **Ms. Gemma Galdon Clavell**, Founder, Eticas.ai, Spain • **Mr. Reza Shokri**, Presidential Young Professor, National University of Singapore, Singapore (remote) **Open discussions** (~30 min)
12:30 – 13:30	**Lunch break**

13:30 – 15:00	**Session 2: Processing sensitive or confidential data securely within less trustworthy digital environments** This session will explore the importance of PETs for securing data processing activities in digital environments that may be considered less secure or trustworthy, including e.g. public cloud services. It will highlight for example encrypted data processing tools that allow data to remain encrypted throughout its lifecycle, ensuring the protection of sensitive information against unauthorised access or other data breaches. Use cases to be discussed could include the use of encrypted data processing tools such as: • Homomorphic encryption to process encrypted e.g. health records for research in a public cloud environment, without decrypting the data. • Trusted execution environments to securely process data in the cloud, while ensuring data confidentiality and integrity. Possible questions for discussions: • What are the practical challenges in implementing encrypted data processing tools in cloud environments, including for small and medium-sized enterprises (SMEs)? • How can we balance the need for digital security with the computational overhead associated with these PETs? • To what extent are cloud service providers and PET developers collaborating and competing, and what are the implications for innovation in PETs? Moderation: **Ms. Clarisse Girot**, Head of Data Governance and Privacy Unit, OECD Directorate for Science, Technology and Innovation Case study presentations (~7 min each): • **Ms. Rina Shainski**, Chairwoman and co-founder, Duality Technologies, United States • **Mr. Katsumi Takahashi**, Chief Security Scientist, Nippon Telegraph and Telephone (NTT) R&D, Japan • **Mr. Robert Pisarczyk**, Co-founder and CEO, Oblivious, Ireland Lead discussants (~5 min each): • **Mr. Adhiraj Saxena**, Senior Products Lead for Technology Incubation, Infocomm Media Development Authority (IMDA), Singapore • **Ms. Laura Galindo**, Privacy Policy Manager, Meta, United States • **Ms. Isabel Barberá,** Co-founder, Rhite, The Netherlands • **Mr. Taylor Reynolds**, Technology Policy Director, Massachusetts Institute of Technology (MIT), United States Open discussions (~30 min)

15:00 – 15:15	**Coffee break**
15:15 – 16:45	**Session 3: Benchmarking the effectiveness of PETs across use cases** This session will address practical benchmarks to assess, compare and communicate the effectiveness of PETs across use cases. It aims to move beyond theoretical constructs, such as the epsilon parameter in differential privacy, to establish common benchmarks that are more actionable and meaningful for policy makers and regulators, as well as for organisations collecting, processing and sharing data. For the latter, practical benchmarks may help for example better evaluate the financial returns on investments in PETs, enhancing the business case for their adoption. Possible questions for discussions: • How can organisations effectively quantify and assess the use of PETs in safeguarding privacy and confidentiality, especially within AI contexts? • What benchmarks, indicators and technical specifications are currently available for evaluating PETs across use cases? • To what extent is there a need for standardised vocabulary and reference implementations to enable internationally comparable benchmarks of PETs? Moderation: **Mr. Allar Laaneleht**, Project Manager, Ministry of Economic Affairs and Communications, Estonia Initial interventions (~7 min each): • **Mr. Baldur Kubo**, Project manager, Cybernetica, Estonia • **Mr. Santiago Zanella-Béguelin**, Principal Researcher, Microsoft, United States • **Mr. Antonio Kung,** CEO - ISO/IEC 27 Editor, Trialog, France Lead discussants (~5 min each): • **Mr. Yves-Alexandre de Montjoye**, Associate Professor, Imperial College London, United Kingdom • **Ms. June Brawner**, Senior policy advisor, Royal Society, United Kingdom • **Ms. Naomi Lefkovitz**, Senior Privacy Policy Advisor, Information Technology Lab, National Institute of Standards and Technology (NIST), United States • **Mr. Winston Maxwell,** Professor, Institut Polytechnique de Paris, France (remote) Open discussions (~30 min)

16:45 – 17:30

Concluding session: Policy and regulatory implications arising from PETs in the context of AI

This session will delve into the policy and regulatory implications that have surfaced from discussions in the preceding sessions and the role of policy measures that complement existing privacy regulation — such as R&D support, education, SME funding, and standard promotion. It will address the extent to which PETs have and should become a strategic policy priority at the highest political levels to enable the next-generation data economy models. It will then conclude with a discussion on potential action points that could be taken forward by governments, regulators as well as the OECD for promoting the effective adoption of PETs.

Possible questions for discussions:

- What are key policy challenges and opportunities in scaling the adoption of PETs across policy domains?
- How can governments facilitate this process in a more strategic and coherent manner? To what extent should PETs play a more prominent role in national AI and data strategies? Or do countries need a national PET strategy?
- How can the OECD better support countries in developing better policies for the effective adoption of PETs?

Panel discussion:

- Moderation: **Ms. Audrey Plonk**, OECD Deputy Director of Science, Technology and Innovation
- **Dr. Mark Durkee,** Head of Data & Technology, Responsible Tech Adoption Unit, United Kingdom Department for Science, Innovation & Technology
- **Mr. Kaarel Sepp**, Project Manager, Ministry of Economic Affairs and Communications, Estonia
- **Ms. Naomi Lefkovitz**, Senior Privacy Policy Advisor, Information Technology Lab, National Institute of Standards and Technology (NIST), United States
- **Ms. Lee Chein Inn,** Deputy Director, Infocomm Media Development Authority (IMDA), Singapore
- **Mr. Vincent Toubiana,** Head of the digital innovation laboratory, National Commission on Informatics and Liberty (CNIL), France (remote)

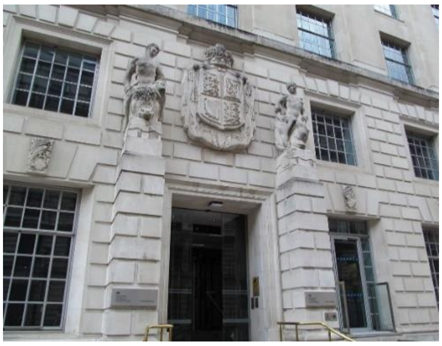
Final comments (15 min)

17:30

END OF WORKSHOP

Informal gathering at the Admiralty (Trafalgar Square, 66 Trafalgar Sq, St. James's, London)

Direction to the Business Events Centre (BEC)



- Directions to the Business Events Centre (BEC) - from Trafalgar Square it is a 5-minute walk. The BEC is easiest to find if you follow directions to the Department for Energy Security and Net Zero (DESNZ) - as they are co-located - on Google Maps.
- DESNZ is located on Whitehall Place, which is the second left when walking down Whitehall from Trafalgar Square.
- **Please mention to security at the main door that you are attending an event at the Business Events Centre** (you will also see directions to the BEC inside the building).
- See https://maps.app.goo.gl/rsWFLFXniov2QZPM9 and photo of entrance above.

Privacy and digital security

- The OECD's configuration of the Zoom service reflects the following privacy and digital security measures:
  - Pre-registration, passwords, and the "waiting room" functions are enabled to prevent unauthorised access to the conference.
  - Specific identity format (country, name) for remote participants for easy control of each attendee in the Waiting Room before admitting them into the meeting.
  - Only the host (OECD) or co-hosts can enable a recording on their local computers.
  - If the conference is recorded, a notice will show on the screen.
  - No chats can be saved, and no private chats are permitted, except with the host or co-hosts.
  - Participants enter the conference call muted and without video showing, unless and until they enable these features themselves.
  - Avoid discussing any highly-sensitive matters and do NOT share your personal invitation link.
- The OECD processes personal data in accordance with its Personal Data Protection Rules: https://www.oecd.org/general/data-protection.htm.
- The OECD will record the workshop and store the recordings on OECD IT systems for the purpose of producing the summary record of the expert workshop, in accordance with the Chatham House Rule. By participating in this workshop, your presence and involvement imply your consent for the workshop to be recorded and the recordings to be used in this manner. For those participating remotely, if you prefer not to be recorded, please mute yourself and turn off your video.
- Similarly, in accordance with the Chatham House Rule, comms activity including social media posts will encompass general publicity material and will not include quotes from the workshop. Images used in publicity and social media will not namecheck any participants. Participants who do not want to be photographed will have the option to opt out during registration on the day.

For further questions please contact:

- **Mr. Christian Reimsbach-Kounatze**, Information Economist / Policy Analyst, OECD Directorate for Science, Technology and Innovation (christian.reimsbach-kounatze@oecd.org)
- **Mr. Shinya Ishikawa**, Policy Analyst, OECD Directorate for Science, Technology and Innovation (shinya.ishikawa@oecd.org)
- Cc: dataandprivacy@oecd.org