



Privacy Enhancing Technologies (PET) in a Omnibus-World

From Compliance to Competitive Edge

Umberto Annino, Expert Strategic Consultant, Aveniq AG

Privacy by Design

- 7 principles
- Originated almost 30 years ago “PET: the path to anonymity”
© Dr. Ann Cavoukian
- Privacy by Design and Privacy by Default:
both mandated in GDPR and swiss DPA explicitly
- PbD would strongly profit from Security by Design
(but here we are)

7 founding principles:

1. Proactive not reactive, preventative not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality (positive-sum, not zero-sum)
5. End-to-End Security (full lifecycle protection)
6. Visibility and Transparency
7. Respect for User Privacy (user-centric)

PET Privacy Enhancing Technologies

Production Grade

- Cryptographic Techniques
 - Encryption
 - (MPC multi-party computation)
 - (FHE fully homomorphic encryption)
- Confidential Computing
TEE (trusted execution environment)
- Differential Privacy
- Synthetic Data

Growing Commercial Adoption

- Federated Learning
- Secure MPC

Emerging / Early Commercial

- FHE Fully Homomorphic Encryption
- ZKP Zero-Knowledge Proofs

The need for PET

- “Treat non-compliance as any other risk”
- PET for risk control (avoid, mitigate)
 - As for risk transfer:
 - cyber insurance companies learned their lesson
 - Difficult to insure (massive) reputational damage resulting from privacy breaches/incidents
- Strategic value of PET:
Enabling activities impossible without PET
(federated learning, synthetic data, x-border research and development ...)
- PET have reached a decent maturation point

PET Reality Check

Adoption Barriers:

- High implementation costs
- Technical Complexity
- Talent shortage
- Lack of standards and interoperability
- Performance overhead

Reality Check:

- Refactoring your codebase/product is not cool (would be, but it's so expensive)
- Technical complexity (in theory, another argument FOR refactoring...), makes implementation expensive
- High costs. It's always the high costs → got better, but still not there
 - “what's in it for me/us?(????)”
 - Information risk is highly abstract

Reality Check Examples

- Twitter/X: internal data access/API breach (2022/2023)
- Meta: GDPR fine (2023)
- 23andMe: Data Breach (2023)
- Clearview AI: Facial image scraping (2020...)
- MOVEit Transfer: mass exploitation (2023)
- NHS and Palantir: opaque data sharing (2021-2024)
- OpenAI: ChatGPT training data & GDPR (2023)
- Microsoft: Cloud intrusion by Storm-0558 (2023) → led to CSRB report
 - SPOF in key management
 - Insufficient SbD posture
 - Weak detection and telemetry design
 - Organizational culture issue
- Microsoft: Corporate Email intrusion by Midnight Blizzard (2023/2024)
- XPLAIN: data leak (2023)
- Google: Maps / Gemini API key escalation

PET Examples (2025/2026)

- Microsoft Azure
 - Confidential VM
 - Azure Confidential Ledger
 - Azure Confidential Inferencing
 - Sovereign Cloud
- Amazon AWS
 - Nitro Enclaves
 - Clean Rooms
 - Cryptographic Computing Stack
 - Sovereign Cloud
- Google Cloud GCP
 - Confidential VM
 - Confidential Space
 - Open-source differential privacy ecosystem
- Europe (companies)
 - OVH Cloud
 - T Cloud Public
 - Infomaniak, Exoscale, Scaleway

Summary / Closing Statements



PET should happen, but it's still slow. Very slow. TOO slow.



PET would help, but it should be deployed. Quickly. Globally. Seriously.



Harm happens at the engineering layer, not the compliance reporting layer

- Omnibus sadly won't help, quite the contrary
 - Failures are of architecture, design, engineering culture, incentive design; not paperwork
 - Organisations will be even less compelled to follow suit
- Simplified compliance = weaker accountability