Enhancing privacy and trust in AI

Riccardo Masucci, Intel @rimaprivacy
Give users more control without shifting the burden to individuals

How to improve Access to Data and foster Automated Decision Making (ADM) while protecting individuals?

1. Acknowledge multiple grounds for processing to improve access to data
2. Embrace risk-based accountability approaches
3. Promote risk-based degrees of human intervention in ADM

See also: Intel AI and Privacy White Paper (October 2018)
Intel Model US Privacy Bill (May 2019, third draft)
We need more encryption and anonymisation to enable AI and to protect citizens

Introducing Privacy Preserving Machine Learning (PPML):

- Pool data without sharing it → *Federated Learning*
- Perform ML while data stays encrypted → *Homomorphic Encryption*
- Collect data with quantifiable privacy protections → *Differential Privacy*

*Used as set of techniques.*

*Performance and usability still to be improved.*
**PPML use case: financial services**

- Bank hires an AI company to develop a fraud detection model;
- Retailers have private data, through **federated learning** the model can be improved and updated;
- To avoid that the model learns about individuals in the datasets, some noise can be added (**differential privacy**);
- To check one transaction, the bank shares data using **homomorphic encryption** with the AI company which sends the result encrypted back, that can be decrypted only by the bank.
Privacy is a key element of Trustworthiness
Ethics can be built on privacy practices

What are possible future directions for tech policy approaches?

1. **Integrated:** trustworthiness encompasses privacy, technical robustness (security, safety, resilience), transparency, ethics...
   - Challenges: siloed regulatory approaches, different metrics, conflicting requirements, no methods for risk composition

2. **Multidisciplinary:** multifaceted issues like ethics require multiple professional skills
   - Privacy experience (privacy-by-design, privacy impact assessment) can be leveraged

3. **Risk-based:** context is key, not all use cases require the same oversight
   - Pre-standardisation/standardisation activities key to map regulatory needs
To summarise:

1. Improve access to data and foster automated decision making while augmenting safeguards by organisations.

2. Promote risk-based accountability and R&D in privacy enhancing technologies like PPML.

3. Follow integrated, multidisciplinary and risk-based policy and regulatory approaches.
THANK YOU!

riccardo.masucci@intel.com
@rimaprivacy