

# The Role of PEC in Recent and Upcoming National Strategies

Presented at WPEC 2024

Angela Robinson

# Increasing international investment in PETs

- UK, US prize challenges for the advancement of PETs
- The United Nations statistics PET lab
  - to make international data sharing more secure by using PETs
  - Pilot project with UK, US, Netherlands and Italy national statistics offices to demonstrate feasibility
- The European Union Agency for Cybersecurity (ENISA) released its PETs readiness report in 2016
- "UK National Data Strategy" document released a few years ago, CDEI PETs adoption guide

## US, UK Collaborate on Prize Challenges for Privacy-Enhancing Technologies

Friday, June 24, 2022

On June 13, US and UK governments **announced** that they are developing prize challenges focused on advancing the maturity of privacy-enhancing technologies (PETs) to combat financial crime. The announcements highlight that up to \$2 trillion of cross-border money laundering takes place each year. The White House explained that PETs could address financial crime through maturing technologies, which allows machine learning models to be trained on high quality datasets, without the data leaving safe environments. PETs also facilitate privacy-preserving financial information sharing and collaborative analytics; allowing suspicious types of behavior to be identified without compromising the pr data between instituti

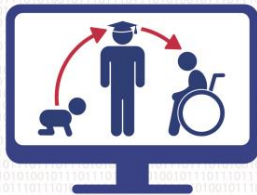
## Gartner Report: Top Strategic Technology Trends for 2021: Privacy-Enhancing Computation

April 2021

For more information on Confidential Computing, check out our blog [here](#).

**"By 2025, 50% of large organizations will adopt privacy-enhancing computation for processing data in untrusted environments and multiparty data analytics use cases."** - Gartner

Gartner has identified privacy-enhancing computation as a key enterprise technology trend for 2021 and enabler for processing and analyzing highly sensitive data. In this new report, **confidential computing** is highlighted as a vital component to unlocking previously




### Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies

Methodology, Pilot Assessment, and Continuity Plan

APPROVED  
VERSION 1.0  
PUBLIC  
DECEMBER 2015

[www.enisa.europa.eu](http://www.enisa.europa.eu) European Union Agency For Network And Information Security



# Executive Office of the U.S. President

- Council of Economic Advisors
- Council on Environmental Quality
- ...
- National Economic Council
- National Security Council
- ...
- **Office of Science and Technology Policy**
- Office of the National Cyber Director
- ...

# Office of Science and Technology Policy

- Advises on all matters related to science and technology, including Federal research development in budgets
- Director of OSTP manages National Science and Technology Council
  - Committee on Technology
    - Subcommittee on NITRD: Networking and Information Technology Research and Development Program
      - Privacy R&D Interagency Working Group

# 2016 National Privacy Research Strategy

- Developed in recognition of challenges to personal privacy from large-scale data collection
- Established objectives for privacy R&D that recognizes
  - Privacy needs of individuals and society
  - Responsibilities of government

# 2023 National Strategy on Advancing Privacy-Preserving Data Sharing and Analytics

- What would a future state of PPDSA adoption look like?
  - Who would benefit?
  - What tools would be adopted?
  - What collaborations would be possible?
  - What policies would contribute to the landscape?
- How do we get there?

# PPDSA Strategy Development

## Inter-agency committee

- NIH US Census Bureau
- DARPA
- NIST CDC
- NSF ...
- VA
- DOE 25 agencies total
- OSTP

## Three subcommittees

- Vision – What does this future PPDSA state look like? What privacy principles guide the landscape?
- Technology – What tools support PPDSA? How do we advance the development of the most promising tools? What are the human factors?
- Adoption – What are barriers to PPDSA adoption? What will advance the adoption?

# Initial challenges

- (Lack of) common language across different agencies
  - Privacy
  - Data sharing vs. Secure computation
  - Conflating PPDSA with PETs
- Varying data types
  - Medical data
  - Genomic data
  - Personal identifiable information
  - Other
- Varying examples PPDSA tools in the wild
  - Pilot programs vs. production level tools vs. Open-source software
  - Information gathering



# Initial recommendations

- Need for taxonomy, better understanding of threat models, risks and privacy harms, ways to measure information leakage
- Sustained R&D in key technologies (DP, SMC, Synthetic data, ..)
- Empowering people to control their data
  - Need effective, usable tools
- Socio-technical and human factors are key to transitioning theory to practice
- Education is key – both on research educational approaches, and educational/awareness activities to reach out to diverse populations

# Privacy-preserving data sharing & analytics

Enables data sharing and analytics in a privacy-preserving manner

Includes approaches that protect

- confidentiality
- disassociability
- unpredictability
- manageability

of individuals and/or groups within a dataset during and after data processing

## Value of PPDSA

- Advance research
- Unlock new insights
- Enable data-driven decision-making
- Catalyze innovation and creativity in a privacy-preserving way



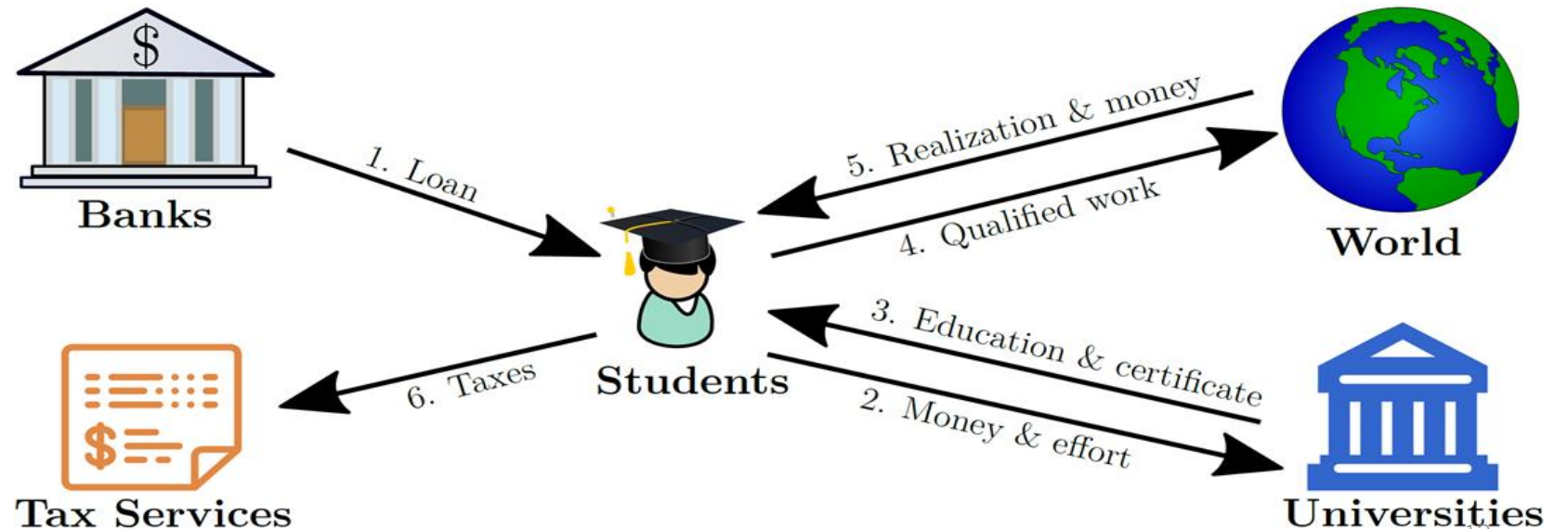
# Use Case: Students' Right to Know

A U.S. Congress bill (2019) mandates the use of SMPC (or equivalent) to estimate the return on investment by students on their college education.

<https://www.congress.gov/bill/116th-congress/house-bill/1565>

The data is distributed across several entities: SSA, Treasury, VA, Universities. Due to privacy concerns, these entities cannot share their data.

Approach: data holders encrypt the relevant data, then use SMPC to calculate aggregate statistics



# Types of PPDSA

- Data masking techniques – anonymization/de-identification, permutation, communication obfuscation
- Differential privacy – centralized DP, local DP, global distributed DP
- Cryptographic algorithms – homomorphic encryption, secure multiparty computation, zero-knowledge proofs, private information retrieval
- Data governance policy management – privacy policy with: access control, anonymization, DP, encryption

# PPDSA Vision

**“Privacy-preserving data sharing and analytics technologies help advance the well-being and prosperity of individuals and society, and promote science and innovation in a manner that affirms democratic values.”**

This vision of the future applies broadly to individuals, groups, and society at large, including industry, civil society, academia, and government at all levels.

# Guiding principles

Guiding principles in support of progress toward achieving the vision:

- PPDSA technologies will be created and used in ways that protect privacy, civil rights, and civil liberties.
- PPDSA technologies will be created and used in a manner that stimulates responsible scientific research and innovation and enables individuals and society to benefit equitably from the value derived from data sharing and analytics.
- PPDSA technologies will be trustworthy and will be created and used in a manner that upholds accountability.
- PPDSA technologies will be created and used to minimize the risk of harm to individuals and society arising from data sharing and analytics, with explicit consideration of impacts on underserved, marginalized, and vulnerable communities.

# Selected recommendations

- 2.a: Develop a holistic scientific understanding of privacy threats, attacks, and harms
- 2.b.1: Accelerate R&D for current and emerging PPDSA technologies
  - Scalability and efficiency
  - Programmability and verifiability
  - Metrics and measurements
  - Fairness, transparency, and accountability
- 2.b.2: Promote future-focused exploratory R&D with transformational goals



# Selected recommendations

- 3.a: Promote applied and translational research and systems development
- 3.b: Pilot implementation activities within Federal Government
- 3.c: Establish technical standards for PPDSA technologies
- 3.d: Accelerate efforts to develop standardized taxonomies, tool repositories, measurement methods, benchmarking, testbeds

# Selected recommendations

5.a: Foster bilateral and multilateral engagements related to a PPDSA ecosystem

- Support international workshops and meetings of experts
- Pursue pilot project and research collaborations
- Participate in bilateral and multilateral fora to advance the responsible adoption of PPDSA technologies

# 2024 National Privacy Research Strategy

“The overarching goal of this strategy is to promote innovative research and technology that protects privacy while advancing the well-being and prosperity of individuals and society.”

To achieve this goals, this strategy identifies the following priorities for privacy research:

- Foster multidisciplinary approach to privacy research and solutions;
- Understand and measure privacy preferences and impacts;
- Develop system design methods that incorporate privacy preferences, requirements, and controls;
- Increase transparency of data collection, sharing, use, and retention;
- Assure that information flows and use are consistent with privacy rules;
- Reduce privacy risks of data analytics and AI.

# Role of PEC community

- Increase awareness of PEC solutions
- Demonstrate interoperability of PEC solutions with other PETs
  - Federated learning with FHE vs MPC vs PSI
- Pilot projects
- Use cases
- Benchmarking, testbeds, taxonomies
- Best practices

**Thank you**

Angela.robinson@nist.gov