What Are Privacy Enhancing Technologies?

ITIF Technology Explainer Series | itif.org

Privacy-enhancing technologies (PETs) are tools that enable entities to access, share, and analyze sensitive data without exposing personal or proprietary information.

How PETs Work

PETs—including differential privacy, federated learning, secure multi-party computation, and fully homomorphic encryption—rely on advanced mathematical and statistical principles to protect data privacy. Such tools make it possible to analyze and collaborate on sensitive datasets while minimizing the risk of re-identification or data leakage.

Why PETs Matter

PETs allow organizations to access, share, and analyze sensitive or proprietary data without exposing it—reducing privacy risks, supporting compliance with data protection laws, and encouraging secure collaboration.

For example, instead of sharing or centralizing data, organizations can use PETs to collaborate while maintaining local control over sensitive data.

In sectors like healthcare, finance, and government, where privacy, regulatory, and security risks can make data sharing difficult, PETs help unlock the value of data, preserve confidentiality, facilitate collaboration, and spur innovation.

PETs also support advances in the development and use of artificial intelligence (AI), which often depend on training models on large volumes of potentially sensitive data. Yet privacy concerns, regulatory requirements (such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA)), and proprietary interests often keep this data siloed.

PET	How it Works	Typical Use Case	Example
Differential Privacy (DP)	Adds statistical noise to data or query results to prevent re-identification of individuals.	Statistical agencies can publish aggregate data (e.g., census statistics) without exposing individual records.	The U.S. Census Bureau applied DP in the 2020 Census.
Federated Learning (FL)	Trains AI models across decentralized sources without moving or sharing raw data.	Research institutions collaborate to train AI models for disease prediction on sensitive data (e.g., clinical records) while keeping the data on-site.	The MELLODDY project enabled 10 pharmaceutical companies to collaboratively train AI drug discovery models without sharing sensitive data.
Secure Multi-Party Computation (SMPC)	Allows multiple parties to compute a joint result (e.g., an average) without revealing their individual inputs.	Universities collaborate on education research by analyzing student performance data from multiple institutions, while keeping individual records private.	The EU's SECURED Innohub uses SMPC for cross-border health data collaboration.
Fully Homomorphic Encryption (FHE)	Allows computations to be performed directly on encrypted data.	A financial institution uses FHE to calculate credit risk scores from encrypted customer data without decrypting it.	Duality's FHE platform enables secure genomic research (e.g., Genome-Wide Association Studies).

Prospects For Advancement

Continued research and development (R&D) is essential to improve the performance and scalability of PETs, some of which remain too computationally demanding or technically complex for widespread use. Progress in algorithm design and hardware acceleration is helping reduce these burdens, but further efforts are important.

While tools to deploy PETs exist, their adoption depends on making them more accessible, user-friendly, and easy to integrate into existing workflows, thereby enabling a wider range of practitioners to use them effectively.

Standardization and interoperability efforts—such as shared protocols and benchmarks—are also critical for consistent, reliable implementation across sectors.

Organizations like the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), and the Organisation for Economic Co-operation and Development (OECD) are working to establish common frameworks to support this goal.

Applications and Impact

PETs are increasingly being tested and adopted in fields like healthcare, finance, and scientific research, where effective collaboration relies on the responsible use of sensitive data.

A compelling example is their use in AI-enabled drug discovery. Developing AI models to predict how potential drug compounds interact with human biology requires access to genetic data, patient clinical data (e.g., electronic health records (EHRs)), and pharmaceutical data. However, privacy and proprietary concerns, intellectual property restrictions, and regulatory requirements often prevent researchers from pooling such data—especially across institutions or borders.

PETs can help overcome data-sharing barriers to enable collaboration and accelerate biomedical innovation. For example, federated learning allows pharmaceutical companies, hospitals, and research centers to collaboratively train AI models without exposing local data. The Innovative Health Initiative's MELLODDY project demonstrated this by enabling 10 pharmaceutical firms to build a shared model to improve drug candidate

PROBLEM: Privacy risks and regulations can prevent organizations from safely using and sharing sensitive data.



ONE WAY FORWARD: Privacy-enhancing technologies (PETs) provide a way to access, share, and analyze sensitive data while helping protect privacy.



Differential Privacy (DP)
Adds statistical noise to data or query results to prevent re-identification of individuals.

Federated Learning (FL)
Trains AI models across decentralized data sources without moving or sharing raw data.

Fully Homomorphic Encryption (FHE)
Allows computations to be performed directly on encrypted data.

Secure Multi-Party Computation (SMPC)
Allows multiple parties to compute a joint result (e.g., an average) without revealing their individual inputs.

screening while preserving proprietary data privacy and confidentiality. This example also shows how AI can be used effectively in sensitive fields, when privacy protections are built in from the start.

Policy Implications

While progress has been made, more can be done to advance the development, deployment, and adoption of PETs—and well-designed policies can play a key role.

1. Support PET Research and Development

- Pass legislation such as the Privacy Enhancing Technology Research Act (H.R.4755, 2023) to fund PET development, deployment, and adoption through the National Science Foundation (NSF), the National Institutes of Health (NIH), and the Department of Energy (DOE).
- Foster public-private partnerships that align incentives between academia, government, and industry to support secure data sharing and enhance transparency and reproducibility.

2. Increase PET Education and Awareness

- Raise awareness through outreach to researchers, legal experts, and IT professionals to demystify PETs and highlight their benefits.
- Fund training programs and workforce development initiatives to build technical PET fluency.

3. Incentivize PET Adoption

- Offer grants, pilot funding, and regulatory sandboxes for PET-enabled projects.
- Develop certification systems (similar to NIST's Cybersecurity Framework) to validate and promote PET-compliant tools and software libraries.
- Encourage adoption through government procurement schemes.

4. Advance PET Standardization and Governance

- Create common standards to ensure interoperability and support widespread adoption.
- Promote alignment through NIST, ISO, OECD, and other multilateral forums.
- Encourage international alignment to harmonize standards for cross-border research and data collaboration.

Recommended Reading

A repository for PETs: https://fpf.org/global/repository-for-privacy-enhancing-technologies-pets/

An introduction to differential privacy: Simson L. Garfinkel, *Differential Privacy* (MIT Press, 2025), https://mitdpbook.com/

Simone Fischer-Hbner and Stefan Berthold, "Privacy-enhancing technologies," *Computer and Information Security Handbook*, Morgan Kaufmann (2017): 759-778.

A repository of PET use cases: https://cdeiuk.github.io/pets-adoption-guide/repository/

A community for open-source PET development and education: https://openmined.org

United Nations PETs Guide: https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf

"Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches," *OECD Digital Economy Papers*, no. 351 (2023), https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/03/emerging-privacy-enhancing-technologies_a6bdf3cb/bf121be4-en.pdf

"Sharing trustworthy AI models with privacy-enhancing technologies," *OECD Artificial Intelligence Papers* (2025): https://www.oecd.org/en/publications/sharing-trustworthy-ai-models-with-privacy-enhancing-technologies_a266160b-en.html

NIST PETs Testbed: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/pets-testbed

A library of open-source differential privacy tools: https://opendp.org

A privacy-preserving platform to advance life sciences research: https://dualitytech.com/use-cases/healthcare-industry/life-sciences/

Recommended Reading Cont.

Alexander Wood, Kayvan Najarian, and Delaram Kahrobaei, "Homomorphic encryption for machine learning in medicine and bioinformatics," *ACM Computing Surveys*, vol. 53, no. 4 (2020): 1-35, https://dl.acm.org/doi/10.1145/3394658.

Peter Kairouz et al., "Advances and open problems in federated learning", *Foundations and Trends in Machine Learning*, (2021) vol. 14, no. 1-2: 1-210, https://ieeexplore.ieee.org/document/9464278

Yehuda Lindell and Benny Pinkas, "Secure Multiparty Computation for Privacy-Preserving Data Mining," *The Journal of Privacy and Confidentiality*, vol. 1, no. 1 (2009): 59-98, https://eprint.iacr.org/2008/197.pdf.