Protecting privacy in practice

The current use, development and limits of Privacy Enhancing Technologies in data analysis

SUMMARY

THE
ROYAL
SOCIETY

Privacy Enhancing Technologies (PETs) are a diverse set of technologies and approaches. In data analysis, they allow the derivation of useful insights from data without requiring full data access.

The scale and rate at which data is collected, used and analysed is rapidly increasing, offering significant new and developing benefits to society and the economy. However, realising the full potential of large-scale data analysis may be constrained by important legal, reputational, political, business and competition concerns. There is a balancing act between realising the benefits of data analysis versus protecting sensitive data and the interests of the individuals and organisations it relates to.

PETs are a nascent but potentially disruptive set of technologies, which, combined with changes in wider policy and business frameworks, could enable significantly greater sharing and use of data in a privacy-preserving, trustworthy manner. PETs could create new opportunities to use datasets without creating unacceptable risks.

The Royal Society's report *Protecting privacy in practice: the current use, development and limits of Privacy Enhancing Technologies in data analysis* reviews a range of PETs, including case studies of specific applications, and sets out the actions necessary to allow us to benefit fully from the development and use of PETs.

To read the full report, visit: **royalsociety.org/privacy-enhancing-technologies**

© filadendron

PETs are developed by different scientific communities and tackle similar problems in different ways

The Royal Society report takes a closer look at a set of fives PETs of diverse nature, defined as:

TRUSTED EXECUTION ENVIRONMENT

Isolated part of secure processors that allow the isolation of secret code from the rest of the software that is running on a system in order to achieve confidentiality of the data. Trusted execution environments are also known as secure enclaves.

HOMOMORPHIC ENCRYPTION

A property that some encryption schemes have, so that it is possible to compute on encrypted data without deciphering it.

SECURE MULTI-PARTY COMPUTATION

A subfield of cryptography concerned with enabling private distributed computations. Secure multi-party computation protocols allow computation or analysis on combined data without the different parties revealing their own private input.

DIFFERENTIAL PRIVACY

Security definition which means that, when a statistic is released, it should not give much more information about a particular individual than if that individual had not been included in the dataset.

PERSONAL DATA STORE

Systems that provide the individual with access and control over data about them, so that they can decide what information they want to share and with whom. Unlike the other four PETs covered in the report, which are tools for privacy-preserving computation, Personal Data Stores are consumer-facing apps and services which can be supported by different kinds of PETs.

Summary table*

	Trusted execution environments	Homomorphic encryption	Secure multi-party computation	Differential privacy	Personal data stores
Type of privacy	• Securely outsourcing to a server, or cloud, computations on sensitive data	• Securely outsourcing specific operations on sensitive data • Safely providing access to sensitive data	• Enabling joint analysis on sensitive data held by several organisations	• Organisation releasing statistics or derived information – generally an organisation that holds a large amount of data	• Individual managing with whom and how they share data • De-centralising services that rely on user data
Privacy risk addressed	• Revealing sensitive attributes present in a dataset	• Revealing sensitive attributes present in a dataset	• Revealing sensitive attributes present in a dataset	• Dataset or output disclosing sensitive information about an entity included in the dataset	• Undesired sharing of sensitive information
Data protected	• In storage • During computing	• In storage • During computing	• During computing	• At point of dataset or result disclosure	• At point of collection • During computing (locally)
Benefits	• Commercial solutions widely available • Zero loss of information	• Can allow zero loss of information • FHE can support the computation of any operation	• No need for a trusted third party - sensitive information is not revealed to anyone • The parties obtain only the resulting analysis or model	• Formal mathematical proof / privacy guarantee • The user can set the level of protection desired, in particular by reasoning about the number of times the data might be queried	• Gives full control to individuals • Removes the risk of attacks on 'honeypots' of centralised data • Analysis can be run locally
Current limitations	• Many side-channel attacks possible	• FHE currently inefficient, but SHE and PHE are usable • Highly computationally intensive; bandwidth and latency issue • Running time • PHE and SHE support the computation of limited functions • Standardisation in progress	• Highly compute and communication intensive	• Noise and loss of information, unless datasets are large enough • Setting the level of protection requires expertise	• Impracticality of individual controlling data sharing with many parties
Readiness level	Product	PHE: Product SHE: Pilot FHE: Research – proof of concept	PSI, PIR: Product Proof of concept – pilot	Pilot	Product
Conditions for implementation		• Specialist skills • Custom protocols • Computing resources	• Specialist skills • Custom protocols • Computing resources	• Specialist skills • Custom protocols • Very large datasets	

KEY

FHE: Fully Homomorphic Encryption **SHE:** Somewhat Homomorphic Encryption
PHE: Partial Homomorphic Encryption **PIR:** Private Information Retrieval **PSI:** Private Set Intersection

* This table is intended as a guide to help understand the five PETs covered in the report in their current state of development as of March 2019. It is not an exhaustive taxonomy of PETs.

Accelerating the research and development of PETs and promoting the development of an innovation ecosystem

PETs are a nascent set of technologies that present the possibility of multiple applications and open up new opportunities for data analysis. However, in their current state a number of these technologies have substantial limitations such as the computing resources that they require, and some are still very much in the research phase. Further research and development is needed in order to start realising the potential of PETs, and to work towards their use on a greater scale.

Funders, government, industry and the third sector can work together to articulate and support the development of cross-sector research challenges, alongside providing continued support for fundamental research on PETs.

There is a considerable market opportunity for PETs. Data-handling companies need to be encouraged to engage with the start-ups and scale-ups developing PETs, supporting research and early trials.

Innovating with PETs in support of human flourishing

The use of PETs does not in itself automatically make an analysis legal, ethical or trustworthy. However, used as part of appropriate governance and good business models, PETs may help the public and private sectors develop solutions that meet their needs and satisfy societal concerns. Government, regulators and civil society should consider how PETs could become part of the data stewardship infrastructure, underpinning governance tools such as 'data trusts'.

© shapecharge

Supporting organisations to become intelligent users of PETs and driving the adoption of PETs

There is a need for government, public bodies and regulators to raise awareness further and provide advice about how suitably mature PETs can mitigate privacy risks and address regulations such as the General Data Protection Regulation (GDPR), with roles for the Information Commissioners Office and the National Cyber Security Centre to provide such guidance. Standards and kitemarks are needed for quality assurance and to increase 'buyer confidence' in PETs.

Government can be an important early adopter, using PETs and being open about their use so that others can learn from their experience. Government departments should consider what existing processing might be performed more safely with PETs and how PETs could unlock new opportunities for data analysis, whilst fully addressing privacy and confidentiality concerns.

Data scientists must receive adequate training and treat the protection of data as core knowledge in data analysis.

> **"The field of PETs development is moving quickly, the technologies are maturing and opportunities to use them are beginning to emerge. Our aim here is to help raise awareness of the potential of these technologies so that we can inspire further research into their development, spurred by identifying the opportunities where they can be put into practice."**
>
> Professor Alison Noble OBE FREng FRS, Chair of the Royal Society Working Group on Privacy Enhancing Technologies, and Technikos Professor of Biomedical Engineering, University of Oxford.

The Royal Society

The Royal Society is a self-governing Fellowship of many of the world's most distinguished scientists drawn from all areas of science, engineering, and medicine. The Society's fundamental purpose, as it has been since its foundation in 1660, is to recognise, promote, and support excellence in science and to encourage the development and use of science for the benefit of humanity.

The Society's strategic priorities are:

- Promoting excellence in science
- Supporting international collaboration
- Demonstrating the importance of science to everyone

For further information

The Royal Society
6 – 9 Carlton House Terrace
London SW1Y 5AG

T +44 20 7451 2500
W royalsociety.org

Founded in 1660, the Royal Society is the independent scientific academy of the UK, dedicated to promoting excellence in science.

Registered Charity No 207043
Issued: May 2019 DES6255

Cover image © from2015.