SLAUGHTER AND MAY/

CLIENT BRIEFING

AUGUST 2021

WILL ADOPTING A PET IMPROVE YOUR PRIVACY?

CDEI PUBLISHES NEW GUIDE ON PRIVACY ENHANCING TECHNOLOGIES

As many organisations struggle to unlock the full value and innovative potential of their data, the Centre for Data Ethics and Innovation (CDEI - see box 'Who are the CDEI?') has been exploring the role privacy enhancing technologies (or PETs) can play in helping to enable data sharing and analysis while protecting the privacy of sensitive data. They have published a PETs adoption guide to help organisations think about how PETs could be useful in their data driven projects, and a blog discussing the guide.

What are PETs?

The term privacy enhancing technologies is a broad definition covering any technical method that protects the privacy or confidentiality of sensitive information. The CDEI's tool contains a section discussing 'what are PETs?' which clarifies that, while PETs could cover anything from simple ad-blocking browser extensions to the Tor network for anonymous communication, the CDEI are focussed on a narrower set of technologies:

- Traditional PETs, which are well established techniques such as encryption schemes and de-identification techniques such as tokenisation; and
- Emerging PETs, which are starting to provide novel solutions to the privacy challenges many face. For this group, the CDEI is focussing on five main technologies: homomorphic encryption, trusted execution environments, secure multi-party computation, differential privacy and systems for federated processing. (See the table overpage)

The guide contains examples of each of these traditional and emerging PETs as well as information on how they can benefit organisations.

PETs: their uses and limitations

Organisations can become too risk averse, and in an attempt to comply with their legal obligations and manage reputational risks they prevent data from being used in ways which may help society (something highlighted in the CDEI's report on public sector data sharing). PETs can, however, help mitigate these risks, thereby unlocking innovation opportunities with data.

That said, they are no silver bullet and PETs have their limitations. For example, they require technical expertise that may be lacking, can be costly to use and can also be misused. One key concern is that they can introduce transparency and accountability risks - they can "enable computation and analysis of data in highly secure environments, which can lead to a false sense of security" and also would not stop unethical data gathering or processing. They should therefore always be used as part of a broader privacy design that includes things like appropriate access control, audit trails and information governance arrangements. Another, more fundamental issue identified by some CDEI stakeholders in an open call that they ran on PETs is a concern around them reinforcing the dominance of certain large technology companies in the private sector, as some PETs require large amounts of data and resources to be effective. Finally, there are also uncertainties around how the use of some PETs should be interpreted in laws and regulations such as the GDPR.

How could the PET guide help you?

Aimed at technical architects and product owners, the guide is primarily a question and answer based decision tree which helps organisations think through which of the PETs mentioned above may be useful in their projects. It also contains a repository of use cases which again may help adoption as organisations can see how PETs can be used in practice.

However, as the CDEI says, the guide "aims not to be overly prescriptive" – it does not, for example, cover all use cases for a PET or guarantee that their use will improve privacy. The information provided is also fairly high level. However, given that the CDEI has found that adoption of PETs by organisations is being hindered (at least in part) by low awareness of the technologies, it may be a useful tool for organisations which are not yet familiar with the different PET options open to them and when they could be used. The guide also points out to general good practice for sharing and processing data which, again, may be helpful for organisations which are not familiar with the main pieces of ICO and NCSC guidance that are available.

PETs and their uses – examples from the Guide

Traditional PETs	Example
Encryption: Encryption is one of the principal security technologies used to protect information. It converts legible data into 'ciphertext' (a representation of the data that is unreadable by human or computer). Decryption requires a key meaning the data is kept secret from everyone who does not have access to this key.	In transit and at rest encryption are mature technologies that are commonly used and should be considered standard practice when sending information over the internet or storing sensitive information.
De-identification techniques: Covers any data transformation or modification that reduces the amount of information about an individual or entity in a dataset, and/or reduces the risk that an individual or entity can be re-identified. They involve direct manipulation of the raw data.	Examples include redaction (e.g. deleting all but the last four digits of a credit card number), tokenisation (e.g. replacing a real value with a randomly generated value) and hashing (applying a function to a value to produce a fixed length value or hash).
Emerging PETs	**Example**
Homomorphic encryption: Enables computation directly on encrypted data (i.e. encryption 'in process' rather than the traditional 'in transit' or 'in rest').	It enables data processing to be outsourced to an untrusted third party or an environment the organisation doesn't trust (like the cloud) as the data remains encrypted throughout.
A trusted execution environment (TEE): A processing environment isolated from a computer's main processor and memory. Communications between the main processor and TEE are encrypted.	A data controller can store data in a TEE to be operated on by an untrusted third party's code also held within the TEE. Processing in the TEE is on unencrypted data meaning it is faster but less secure then homomorphic encryption. TEEs are also hardware -based meaning they need patching and there is no industry standard for interacting with them.
Multi-party computation (MPC) protocol: Enables a function taking input from multiple parties to be jointly computed (although parties keep individual input confidential), often by fragmenting the data over multiple networked nodes. Each node computes an unintelligible 'shard' and the outcomes are aggregated into a final result.	It enables parties to input and process data that they want to keep confidential (e.g. employees who want to determine their average salary without disclosing their individual salaries). There are a number of limitations (e.g. sometimes the output from an MPC protocol can be used to infer information about the input data) listed in the guide.
Differential privacy: A definition of privacy requiring that the output of any statistical analysis does not reveal any information specific to an individual data set (e.g. by adding mathematical 'noise' to the input or output data). The amount of noise must be carefully chosen - too little and the dataset will not be private, too much and it will be too inaccurate to provide statistically valid information. This balance is called the privacy-utility trade-off.	The US Census Bureau used differential privacy to protect the privacy of those who participated in the 2020 census. However, critics said it produced inaccurate data - see this article for more information.
Federated analytics: A paradigm for executing a computer program against decentralised data. A party uploads the program to the server/device containing the data, executing it on the data in situ, and sending the results back to the originating party (who never sees the data). The data never leaves the device as only model weights are communicated.	Federated learning, training a machine learning model on distributed datasets (i.e. training local models directly on users' devices) is a subset of federated analytics. Because information can be inferred from the weights, mechanisms such as differential privacy, are often used as well.

Next steps

The guide was published in BETA phase and the CDEI has requested feedback and additional use cases to help improve it. We therefore expect an updated version to be released in due course. The CDEI has also said that it is working on a number of other projects to help manage some of the limitations PETs face. For example, as mentioned in the CDEI's recent two year review, it is looking at ways to support responsible data access and sharing and is working on a range of projects related to responsible data governance which should all help create the right environment to increase the adoption rate for PETs. In addition, PETs are high on the ICO's current agenda. The ICO published a call for views on its new 'Anonymisation, Pseudonymisation and PETs' guidance which will look at how PETs and anonymisation should be interpreted in regulation and the role of PETs in safe data sharing. It also mentioned PETs in the 'Data Protection by Design and Default' section of the Guide to Data Protection (which discusses the ICO providing further PET guidance in the future) and recently announced (July 2021) that its regulatory sandbox has re-opened with a new area of focus for 2021-2022 on products and services using innovative technologies such as PETs.

In terms of practical next steps, market commentators have told us that while the CDEI report gives a good overview, now is the point at which we need to see more of these techniques actually being used rather than just discussed.

Who are the CDEI?

The Centre for Data Ethics and Innovation (CDEI) is an independent advisory body set up and tasked by the UK Government to advise on how the UK can maximise the benefits of data-driven technologies.

It "aims to bring people together from across sectors and society to shape practical recommendations for the government, as well as advice for regulators, and industry, that support responsible innovation and help build a strong, trustworthy system of governance." See https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation

CONTACT

ROB SUMROY
PARTNER
T:020 7090 4032
E: Rob.Sumroy@slaughterandmay.com

NATALIE DONOVAN
PSL COUNSEL
T:020 7090- 4058
E: Natalie.Donovan @Slaughterandmay.com

London
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Brussels
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
T +852 2521 0551
F +852 2845 2125

Beijing
T +86 10 5965 0600
F +86 10 5965 0650

Published to provide general information and not as legal advice.
For further information, please speak to your usual Slaughter and May contact.

www.slaughterandmay.com