CASE STUDY

# Privacy Enhancing Technologies in Practice

Newton Gateway to Mathematics

## BACKGROUND

One of the most valuable assets an organisation possesses is its data, yet there are many reasons why sharing aspects of this data might be desirable. Regulators or governmental organisations may require access to data, for example to detect crime, and pooled data may provide insights organisations cannot gain from their own data sets alone. The last few years have seen the emergence of technologies which allow for the secure collection, sharing, processing, and storage of data without the downsides of reducing privacy of users, or compromising corporate security. These Privacy Enhancing Technologies (PETs) help to form the basis of various new ways of doing business, with many being highlighted in recent industry reports as opening up new ways of exploiting data.

From November 2020 to January 2021, the Newton Gateway, along with Professor Nigel Smart and in collaboration with the Digital Catapult, hosted a virtual event series recognising the need to help business and industry find effective ways to utilise the new PETs. Consultation with experts had identified a need to facilitate a greater understanding of these technologies amongst end-users, confirming the need to develop and run this short event series.

## CHALLENGES

Realising the full value of the data held by an organisation may require comparison or computation against data held by others. Unfortunately sharing data is one of the hardest things for companies to do, because of the perceived commercial and legal risks. Even within a single organisation, sharing data can be considered to create large security or privacy risks.

PETs can achieve what at first sight seems impossible: they provide ways of processing data without seeing it. Though highly counterintuitive, these technologies open up new and ground-breaking ways of working. To provide organisations with knowledge of PETs, and thus enable the trustworthy use of data, the UK Government's Centre for Data Ethics and Innovation launched a website to provide organisations with knowledge of PETs. As highlighted in the Royal Society report on PETs, organisations are keen to understand how sensitive data can be used for public good, while protecting the privacy of individuals.

The Newton Gateway event series recognised the need to further support businesses and industry in finding effective ways to utilise the new PETs, facilitating greater understanding amongst end-users without them necessarily needing to know exactly "how" the technologies work. The events were of interest to anyone in business and industry who has a need to share and/or process data securely, as well as those focused on corporate cyber security.

> ***"The PET series of interviews I ran in a virtual casual discussion format, was a welcome break from the usual Zoom presentations we all "zoom" out of in these lockdown times. We had five stimulating discussions with industry leaders (in the technology, in the user sphere and from investors)."***
>
> **NIGEL SMART**
> KE LEUVEN

CASE STUDY

# Privacy Enhancing Technologies in Practice

Newton Gateway to Mathematics

## ACTIVITIES

Nigel Smart hosted the event series, which was co-convened with the Digital Catapult and ran across five sessions. Sessions 1-3 featured talks from experts developing some of these technologies. Dan Bogdanov of Cybernetica discussed multiparty computation, a sub-field of cryptography which has been applied to many use cases with potential applications in long-term shared data governance. Rand Hindi of Zama covered the area of Fully Homomorphic Encryption schemes, a form of encryption which allows computations on encrypted data. In the third session, Eli Ben Sasson of Starkware focused on Zero-knowledge proofs, a cryptographic technology that allows one party to prove a statement to another, without the need to reveal the actual values being proven.

The talks highlighted why PETs can be trusted and how they enable the value in data to be unlocked; without needing to compromise on the privacy or security of the data. They also highlighted how users can go about exploring and running tests on the technologies, across a range of potential application domains, from inter- to intra- company security.

Session 4 drew on the perspectives of PET end-users, including Mark Craddock of GCATI and Matt Lowe of the Financial Conduct Authority (FCA). In Session 5 Lawrence Lundy of Lunar Ventures, Yuval Shachar of Team8 and Alex van Someren of Amadeus Capital Partners discussed the challenges and opportunities for investors in PET technologies.

## IMPACTS

The series provided a platform to highlight the capabilities of PETs and enabled key stakeholders — technology experts, end-users and investors — to share knowledge and experience with others. The importance and popularity of such technologies was demonstrated by the volume and calibre of participants, and through the vast amount of activity on social media after each event.

A key message is the need for training in PETs, which can be a big impediment to the uptake of technology. Even highly skilled mathematicians and statisticians employed by an organisation may not necessarily be able to correctly implement new techniques. Talks also highlighted that Big Data, which is owned by private companies, needs to be made more accessible to potentially be used by the public sector, without compromising privacy.

The FCA talk focused on the crime of money laundering and identified areas to be focused on to tackle it: how do we verify that individuals are who they say they are; how can industries, regulators and governments work together to help solve the issue of money laundering; and how do we share data with the regulators and institutions so that we can better detect money laundering?

Finally, the session on investor perspectives gave insights into near-term future opportunities and developments for PETs and highlighted that, in order to make way for innovation and facilitate progress, regulators could make exceptions in regulations to allow experimentation.

> ***All five discussions illuminated how PET technologies are being used, and can be used, to address significant societal challenges. We heard about applications ranging from the specific (such as anti-money laundering initiatives) through to the generic (how to evaluate a neural network on encrypted data). More importantly, we explained how one turns technological ideas into companies, products and services in the real world; and looked at the barriers which can stop the transfer.***
>
> **NIGEL SMART**
> KE LEUVEN

> ***Unlocking knowledge around better data sharing technologies is going to be the key to having a successful advanced digital economy in the future***
>
> **ROBERT LEARNEY**
> DIGITAL CATAPULT

**Newton Gateway to Mathematics**
Isaac Newton Institute,
20 Clarkson Road Cambridge, CB3 0EH, UK
tel: 01223 765580 email: gateway@newton.ac.uk
web: http://gateway.newton.ac.uk

MAR 2022