Using MPC technology to enhance privacy in data sharing

The encryption-based Multi-Party Computation (MPC) technology enables data collaboration without the parties actually sharing the personal data. By **Laura Linkomies**.

A user case from the Netherlands under the aegis of the Data Sharing Coalition brings positive news for those grappling with data sharing challenges. Private, public and the civil sector actors collaborated in a project that was based on cross-domain data sharing for the purpose of preventing and monitoring human trafficking. In this case, information obtained by law enforcement agencies of victims of forced prostitution was processed together with information from victims obtained by NGOs. The Sustainable Rescue Foundation (an NGO), Roseman Labs and others worked with privacy experts at Pinsent Masons to develop a system based on MPC (Multi-Party Computation) technology to help overcome the privacy law challenges so that sensitive data could be processed in confidence.

The main challenge in this use case was to enable collaboration between the parties without having to share sensitive personal data. The law enforcement agency has a list of names of individuals who are potentially engaged in criminal activities. A small number of people are put under observation. The NGO's also hold a list of names – that is those of the informants - and wants to ensure that none of the informants is put under observation by the law enforcement agency. How can the parties achieve this, if they are unwilling (or, not allowed) to share these lists with each other? An additional complexity is that not all names are spelled correctly.

MPC is based on four decades of academic research in theoretical cryptography. It enables several participants to perform a computation on their joint input data, while their inputs remain mutually private (the input from each participant remains secret to all other participants), and without involving a trusted third party.

"In theory, MPC technology has been available for quite some time," Andre Walter, Head of Data Law Solutions at Pinsent Masons Netherlands said. "It is not just about encrypting data but about the ability to process encrypted data without lifting the encryption at any moment in time".

In this user case, Roseman Labs, a high-tech software company that enables organisations to collaborate on privacy sensitive data through MPC, ran the process on encrypted data in real time. The process mitigates the risks because no personal data is exposed. Only the end result, in this case a short list for the law enforcement agency is revealed to the agency.

Ian Wachters, Commercial Officer at Roseman Labs, explained that each bit of data is divided into separate signifiers (numbers) which will reconstruct the information only if put together. The data is held on three separate servers and no one has access to these three servers in parallel.

> The main challenge in this use case was to enable collaboration between the parties without having to share sensitive personal data.

"MPC is the most powerful privacy enhancing technology that is available," Wachters said. "The technology is now at a tipping point of being practical because of recent mathematical innovations and faster computers and networks. It can therefore now be applied to everyday problems."

But given that the technology is not something you come across every day, how were the NGOs convinced that their users' data would be safe?

"We explained the process thoroughly. Then Roseman Labs assisted the organisations in running an 'MPC ceremony': three laptops, located at three different cities in the Netherlands, ran Roseman Labs' MPC protocol over the Internet, " Walter said.

Each laptop was provided with a list of the individuals' data the organisation had in that city. A Roseman Labs person assisted the organisation during execution of the protocol.

"User trust is paramount and it is very important that all concerned are kept informed," Walter said.

MPC and GDPR-compliance

"Although under a strict interpretation of GDPR the encrypted data is still not considered anonymous, MPC provides a tremendous help in complying with GDPR principles such as purpose limitation and data minimisation" Walter said.

The outcome of an MPC ceremony is defined beforehand, and that way the algorithm, and with it the processing of the data, is run to achieve only the envisioned purpose.

In terms of data minimization, all data provided by the participating parties is encrypted at the source and hence not visible to anybody else during the process. Only the end result is revealed, and only to the designated party. MPC therefore enables collaboration where parties would not previously have trusted each other.

"MPC does not try to avoid the GDPR but can be used to enhance compliance. We take the same strict view as the Netherlands' DPA – encrypted data is not anonymous data as it can be reconstructed. Therefore, the GDPR still applies," Wachters said. MPC technology makes possible processes that previously were not because the parties would not trust each other. Now when using MPC technology, they do.

EDPB promotes this type of technology

EU DPAs acknowledge that technical measures may supplement other safeguards for data transfers to third countries, and they say that new technologies may still emerge.

The European Data Protection Board said in its 21 June 2021 guidance on international transfers that as a supplementary measure to a data transfer, split or multi-party processing is acceptable. Its use case (number 5 in annex 2) proposes the following scenario:

"The data exporter wishes personal data to be processed jointly by two or more independent processors located in different jurisdictions without disclosing the content of the data to them. Prior to transmission, it splits the data in such a way that no part an individual processor receives suffices to reconstruct the personal data in whole or in part. The data exporter receives the result of the processing from each of the processors independently, and merges the pieces received to arrive at the final result which may constitute personal or aggregated data."

Multi-party computation can be used as a technical supplementary measure if there is no evidence of collaboration between the public authorities located in the respective jurisdictions, the DPAs say.

Going forward – an eye on international transfers

MPC solutions are ready to be used commercially. In fact, big players such as Coinbase and PayPal are already deploying MPC where they need extra security and privacy for cryptographic key management.

Rosie Nance, Practice Development Lawyer at Pinsent Masons said she is very excited about the technology's potential to overcome challenges around *Schrems II*, data localisation laws, and other restrictions around sharing certain types of data.

"The solution could enable collaboration and data sharing that would otherwise not be possible due to strict data localisation laws, *Schrems II*, local restrictions around data used for purposes like law enforcement, or a combination of all three of these factors. As lawyers based in the EU or UK, shifting processing to the EU or UK might seem like a solution to the challenges that arise on projects requiring international data sharing – and that would generally address *Schrems II* concerns. However, global organisations face complex and sometimes conflicting compliance requirements, and that would only deal with one piece of the puzzle."

Nance foresees potential for further application of the technology in the financial sector, particularly in fraud prevention. Wachters agrees: "Anti-money laundering is a good example. If a bank only monitors their own transactions, it may not get a clear picture of what is happening. With the help of MPC, it can work with other collaborators to flag those that fulfil fraudulent criteria. Those transactions will then be looked at but only within that organization – so data is not shared with third parties."

Similarly, MPC technology could aid insurance companies to share their loss data in a privacy friendly way in order to better understand risk profiles, Wachters said. Other potential uses could be found in marketing. For example, two retailers with different product categories but both running loyalty schemes could understand their consumers' behaviour better as micro-segments can be created without actually sharing personal data.

MPC can also be used in the health sector and Wachters says this is very much a focus of Roseman Labs. The technology becomes useful when different health providers need to collaborate but data cannot be shared due to compliance reasons. For example, several hospitals can collaborate in a clinical study without revealing patient records to each other, and only reveal the conclusions of the study. Another question is how this technology could be explained to patients in a health system context, as the use of MPC would most likely require their informed consent.

Other possible uses could be in genetic testing to let people check their own genetic profile, or keeping bids private in sealed-bid auctions.

Roseman Labs stresses that MPC provides both the strongest technical and organisation safeguards as required under the GDPR.

However, MPC will not solve every compliance challenge around sharing personal data: "MPC is not a silver bullet but it provides some legal certainty for data used for these types of data collaborations," Walter said. "Now that the EU Data Governance Act is about to be adopted, there will be increased pressures for data sharing and this needs to take place in a secure environment."

INFORMATION

rosemanlabs.com/assets/video/explainer_video_mpc.mp4
www.qredo.com/blog/what-is-multi-party-computation-mpc
www.fireblocks.com/what-is-mpc/
datasharingcoalition.eu/app/uploads/2021/04/data-sharing-canvas-30-04-2021.pdf

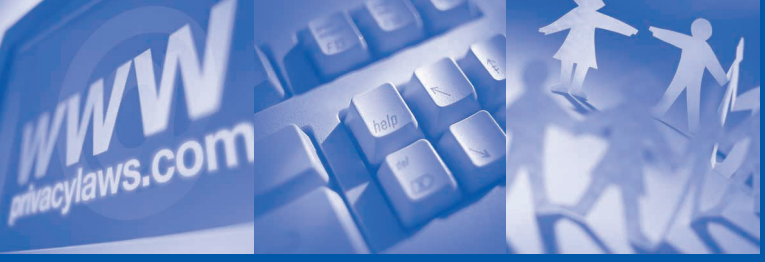
DATA SHARING COALITION

The Data Sharing Coalition, an international project operating in the Netherlands, encourages new members to join. Participants are expected to contribute to the work by

- Contributing to the definition and realisation of cross-sectoral use cases of data sharing
- Providing input and expertise to determine the harmonisation potential between data sharing initiatives (Data Sharing Canvas)
- Driving knowledge sharing about (cross-sectoral) data sharing.

The initiative started in January 2020, after the Netherlands' Ministry of Economic Affairs and Climate Policy invited the market to seek cooperation in pursuit of cross-sectoral data sharing. The Data Sharing Coalition, supported by the Ministry, was started as a direct result.

See datasharingcoalition.eu/joining-the-data-sharing-coalition/



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Now 157 countries: 12 data privacy laws in 2021/22

Sri Lanka, Oman and the United Arab Emirates have adopted new data protection laws in 2022. **Graham Greenleaf** reports on recent developments.

Despite the Covid pandemic, countries across the globe have continued to enact data privacy laws. At the start of 2021, 145 countries had done so,[1] but in the year since then a further 12 countries have enacted such laws, giving a total of 157 by mid-March 2022. As has become familiar, most of these laws are influenced substantially by the EU's GDPR, but with many variations in such implementations. The

Continued on p.3

Apple AirTag debacle shows we need to diversify privacy

Diversifying privacy means more than diversifying product development and privacy teams. We need to broaden the aperture and centre marginalized voices. By **Abigail Dubiniecki**, Privacy lawyer and consultant.

"Apple's website states that 'privacy is a fundamental human right,' but one of its new products apparently didn't get the memo."[1]

Apple has long made privacy a key brand differentiator, with cutting-edge privacy engineering baked into its offering. Yet the PR fallout from privacy risks that surfaced soon

Continued on p.9

Issue 176 **APRIL 2022**

INTERNATIONAL report

ISSUE NO 176 APRIL 2022

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS

Katharina A. Weimer
Fieldfisher, Germany

Nicole Wolters Ruckert and Tim Sweerts
Allen & Overy, Netherlands

Elizabeth Canter and Natalie Dugan
Covington & Burling, US

Abigail Dubiniecki
Independent privacy lawyer and consultant, Canada

Gabriela Kennedy and Joshua T. K. Woo
Mayer Brown, Hong Kong

Nada Ihab
Access Partnership, UK

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

The many faces of AI

Recently, Italy's Data Protection Authority imposed a fine of €20 million on Clearview, and banned any further processing of citizens' facial biometrics (p.11).

Clearview has also been the target of regulatory action in the UK, France, Australia and Canada. The UK ICO conducted a thorough investigation into Clearview's processing of personal data in cooperation with the Office of the Australian Information Commissioner culminating in ordering the company to stop processing data. In France, the DPA has taken similar action.

Although the company has been heavily criticised for not having an adequate legal basis for its processing, now in Ukraine this facial recognition technology has been used to identify Russian soldiers that have died in Ukraine. While the power of AI can be advantageous in reuniting refugee families or identifying the dead, what happens if the database falls into the wrong hands?

I would be interested in hearing how your company is reacting to the war in terms of data transfers to and from Russia, and processing operations in both countries. Please let me know if you can share your experience with *PL&B* readers.

There is now positive news regarding the EU-US data transfer situation – the parties have announced that they have agreed, in principle, a new framework (p.31). The teams of the US Government and the European Commission will now continue their cooperation with a view to translate this outline arrangement into legal documents that will need to be adopted on both sides to put in place this new Trans-Atlantic Data Privacy Framework. For that purpose, these US commitments will be included in an Executive Order that will form the basis of the Commission's assessment in its future adequacy decision, the EU says. Both sides want to avoid a *Schrems III* banning judgement from the Court of Justice of the European Union.

This is welcome progress as it is expected that the final agreement will be ready this Spring. In the meantime, another three US states, Colorado (p.13),Virginia and Utah (p.15) have adopted data privacy laws (the California Consumer Privacy Act was adopted in 2018).

Internationally, Professor Graham Greenleaf reports (p.1) on 12 new data privacy laws in 2021/22, including the more recent ones in Oman, Sri Lanka and the United Arab Emirates.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 168+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 168+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

> *PL&B International Report* is a very useful and business-friendly publication that allows our team to easily and frequently keep up with developments in countries outside our jurisdictions of activity.
>
> **Magda Cocco and Inês Antas de Barros, Partners and Isabel Ornelas, Managing Associate, Information, Communication & Technology Practice, Vieira de Almeida, Lisbon**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.