Federal Register Notice 87 FR 35250, https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies, June 9, 2022

Request for Information (RFI) on

Advancing Privacy Enhancing Technologies

Ixup Solutions

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.

Office of Science and Technology Policy

Friday 8 July 2022

Reference: Request for Information on Advancing Privacy-Enhancing Technologies

Thank you for the opportunity to make comment on the commercial application of Privacy Enhancing Technology.

We are a small Australian Privacy Enhancing Technology development company specializing in encrypted data solutions, specifically to address collaborative data requirements across a variety of sectors, including Government, Banking, Insurance, Gaming, and Loyalty programs.

To that end, our commentary is specifically aimed at Category 3 of the topics requested by this RFI.

This is an important initiative being undertaken, and we wish you a very productive outcome.

If we can provide any further information or assistance, we would welcome an approach from the OSTP.

Yours sincerely,

Peter Hong
General Manager, Government
Ixup Solutions
Sub Base Platypus
Suite 1004, 118 High St.
North Sydney, NSW 2060
AUSTRALIA

Mobile: Email:

The volume of data that is being created and used continues to grow exponentially. In 2020, the world produced 64.2 zettabytes of information with that expected to triple by 2025. At the same time, there has been an increased focus on data protection and privacy that has resulted in encryption becoming the default for the storage and transmission of data.

The convergence of these two trends has created new challenges for organisations. Everything from digital transformation efforts and the growth of open data and online gaming to the increased oversight by regulators when it comes to the protection and use of personal data relies on the ability to understand data from multiple sources. But when that data is encrypted, the ability for it to be read and used can be hampered.

Encryption's purpose is to prevent the unauthorised use of information. This makes sense when data is being stored and moved. But what about when we want to use it? The typical approach has been to decrypt data when it needs to be transacted or analysed.

Encryption has significantly reduced the risk of doing business online at scale, improving productivity while also protecting sensitive commercial and personal information. But when we want data to be put to work it needs to be decrypted so that computers can transact, compute, analyse or report on that data. This is the weakest link in your data security chain but it's also where we turn data into real business value.

With about 70 per cent of the world's GDP digitised, securely managing data through the entire value chain is critical. That means industries as diverse as governments through to esports need to find ways to gain value from encrypted data. This is what homomorphic encryption makes possible. It is an enabler of consumer data rights, business integrity, compliance, and social impact, allowing encrypted data to be securely computed, analysed, processed, and reported on.

Encryption uses a public key to encrypt data so only someone, or a machine, with a matching private key can decrypt the data. Homomorphic encryption – "homomorphic" means "same shape" – uses algorithms to maintain the relationships between elements in data, which in turn, allows for encrypted computation. This supports businesses in their governance, risk, and compliance (GRC) obligations as they can share and process data without weakening security.

The resulting computations are also encrypted and can only be revealed using the secure, private key. This level of security means value can be added to data sets without compromising the integrity or privacy of the source data. The enriched data can be tracked, traced, and audited, ensuring a continuous chain of custody, building trust and provenance at the same time.

With environment, social and governance (ESG) now a major issue for boards, and increasing oversight from regulators all over the world, ensuring the confidentiality and integrity of data is vital. Homomorphic encryption is a game-changer that will enable organisations to protect data through its entire value chain at scale and in a form that supports large batch processing or real-time transaction processing, but organisations need to invest in the right tools and work with experienced partners.

As more organisations use public and private cloud solutions, privacy enhancing technologies like homomorphic encryption will become increasingly important.

For example, an organisation may choose to store an encrypted, sensitive data set on a cloud service and perform some calculations with that data. At no point does the operator of the cloud service decrypt the original data or the result of the calculations. Both the actual calculations and the result remain encrypted and can only be accessed by someone with the decryption key.

As data privacy legislation becomes more prevalent – Gartner says that by 2023, 73 per cent of the world will be subject to privacy rules such as the European Union's General Data Protection Rules, the Australian Privacy Principles, and others – ensuring the confidentiality and integrity of personal data through the entire value chain is a significant compliance issue.

Securing private information has, up until now, been the responsibility of each organisation, but these regulatory changes are extending that responsibility across enterprises and industries – and businesses are needing to turn to privacy-enhancing technologies to fill the gap.

For example, **IXUP is collaborating with Microsoft to enhance the privacy of gaming operators to protect vulnerable gamblers and for sporting bodies to prevent impermissible betting (sports integrity)**. By ensuring information such as self-exclusion data always remains safe, gamblers will be able to protect themselves from the effects of gambling while enabling service operators to ensure vulnerable people are removed from marketing campaigns and prevented from betting.

This, we believe, was the first implementation globally of homomorphic encryption turning a privacy challenge into a social impact benefit.

More information is available here:

Information for Regulators PlayPause v1.2.pdf

https://ixup.com/press/taking-responsible-gaming-and-sports-integrity-to-a-new-digital-level/

A very similar model could be easily deployed to protect the privacy of individuals in any other register, including, for example, a gun owners or gun licensing register where checks may be required across disparate data sources (law enforcement, health, education, social services for example) before a license is granted.

Creating new approaches and extending the reach of financial audit processes also promises a long overdue positive change. Repurposing audits to include new service offerings such as the audit of machine learning algorithms or arrive at a realistic value for an IPO valuation using the measure of interest gleaned from a company's own website. These are but two possibilities that would enhance existing offerings and help to create greater value for customers by the addition of complimentary offerings to the financial audit process.

Privacy enhancing technologies could provide an ideal technology platform to assist accountancy and financial services providers as well as fintech technology vendors an opportunity to rethink traditional audit and accountancy products and reinstitute trust in audit and assurance.

In the world of Open Banking/Open Finance, consumers demand, and deserve, ultimate privacy in all transactions that share their personal identifiable information. PET, and in particular homomorphic encryption, can underpin the integrity and security of those transactions and computations without compromise – the encrypted data cannot be reverse engineered to reveal the original information unlike hashing.

For more detail of this Use Case, please refer to Privacy Preserving Homomorphic Encryption for Audit Practice v2.pdf

As you know, organisations are under increasing pressure and scrutiny to ensure they protect sensitive data. Homomorphic encryption enables them to maintain security even when using data. The days of needing to decrypt data to extract value from it will be behind us as this proven and cost-effective technology helps keep personal data private.

End of Submission