VANTEUM galois inpher

Introduction

We would like to commend the Australian Senate for their forward-thinking commitment to the Australian Innovation and Financial Services ecosystems by establishing the Select Committee on Financial Technology and Regulatory Technology. We also applaud the committee's consulting with various stakeholders and encouraging the Australian public to make submissions.

Our consortium brings to the committee unrivaled access to global experts in privacy and information security technologies, supported by world leading research & development and hands on experience in the implementation of financial and regulatory technology best practice. Established by Sydney based consulting firm, Vanteum, our consortium's submission focuses on the adoption of Privacy Preserving Protocols (PPP), which enable tremendous value to be unlocked from data (both organisational and personal) whilst guaranteeing the privacy and security of this data.

PPP technologies have been proven to unlock tremendous value for government and regulators, banks and other financial institutions. We refer the reader to the United Nations Handbook on Privacy Preserving Computation Techniques, co-edited by a member of our consortium, for a detailed discussion of these technologies, their applications, and related international standardisation efforts. Uniquely PPP techniques allows data to be analysed while still encrypted, significantly reducing the risk of a data breach and allowing organisations to access data sets previously unattainable due to privacy concerns and commercial sensitivity.

Through application of these capabilities, it is possible for AUSTRAC and other regulators to identify illegal money flows in banking across multiple institutions without the respective institutions needing to disclose their transactional data to each other or the regulator. There are also applications in detecting incidences of motor vehicle insurance fraud across multiple insurers and in a recent submission by Vanteum and Galois to the Department of Health as part of their Data matching bill, Vanteum and Galois proposed a way to address up to $600 million worth of fraudulent Medicare claims without needing to move, disclose or unencrypt sensitive data on individuals from multiple Government Departments[1].

At the international level, the UK Financial Conduct Authority ("FCA") recently hosted a Tech Sprint to support the development of privacy-enhancing analytics in financial enforcement.[2] Inpher, a US-based cryptography and machine-learning company, successfully demonstrated the application of secure Multi-Party Computation (MPC) to combat financial crime, detect fraudulent activities, and prevent money laundering whilst adhering to strict privacy law requirements.[3]

Inpher's MPC technique, called 'Secret Computing', transforms plaintext data into random auxiliary numbers to enable secure collaboration across siloed departments, industries, and

---

[1]Vanteum and Galois submission on the Department of Health Data matching bil: https://consultations.health.gov.au/provider-benefits-integrity/draft-health-legislation-amendment-data-matching-b/supporting_documents/Submission%2012%20%20Vanteum%20%20Galois.PDF

[2] UK Financial Conduct Authority, *2019 Global AML and Financial Crime TechSprint* (Held on Jul. 29, 2019 to Aug. 2, 2019), https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint

[3] Inpher, *Inpher Wins People's Choice Award at FCA TechSprint* (Aug. 9, 2019), https://www.inpher.io/news/2019/8/9/inpher-wins-peoples-choice-award-at-financial-conduct-authoritys-2019-tech-sprint.

jurisdictions—without disclosing or transferring any personal information between parties. Inpher actively advocates for policymakers to explore and support privacy-preserving, cryptographic technologies as a safeguard against preventable security risks caused by data centralisation.[4] As policy and regulatory debates continue to shape modern data privacy laws, MPC and advanced "encryption in-use" technologies can allow businesses and regulators to make intelligent data-driven decisions while protecting data residency and individual privacy in a transformative regulatory environment.

The development and application of these capabilities in and across, government, financial services and regulators has a significant opportunity to generate billions of dollars for the Australian economy, establish Australia as a leader in this field and create an environment where the protection of citizen data is never compromised. With the right levels of government and regulatory support, Australia could leverage the capability built in this area and develop this as an export for the $127BN emerging global Regtech sector.[5]

[4] U.S. House Financial Services Committee, *AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers* (Oct. 18, 2019), Testimony of Inpher CEO Jordan Brandt, https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-wstate-brandtj-20191018.pdf

[5] Juniper Research on Global Regtech Spending https://www.juniperresearch.com/press/press-releases/regtech-spending-to-reach-$127-billion-by-2024

About us

Vanteum, Galois, and Inpher are a global consortium comprised of data governance and data security experts who have developed and leveraged the latest secure data collaboration technology in a range of government, defence and financial services settings.

This has included work on Open Banking internationally, the Consumer Data Right in Australia and helping both Financial Services regulators and banks internationally to leverage datasets across multiple organisations to address problems such as fraud, money laundering, and terrorism financing amongst others.

Specific people involved:

Alistair Muir is the Chief Executive Officer of Vanteum, a Sydney based consultancy.
Alistair has extensive experience in data partnerships and data sharing arrangements across both the private and public sectors in Australia that balance the need for commercial outcome with the security and protection of individuals' data. These include extensive experience in advising companies on the Consumer Data Right in Australia and Open Banking domestically and internationally. Alistair has also advised CSIRO, Data61 and several research teams in universities in every Australian state/territory on the use of data to solve industry problems.

Tim Scott is an Advisor to Vanteum and is the former Head of Strategic Engagements with IXUP. Tim has worked extensively in the enterprise technology space and experience from his time at SAP, IBM, Oracle and Versent.

Frank McKenna is a Senior Strategy Consultant at Vanteum and is the former Chief Product Officer at Data Republic, which is an Australian Headquartered Data exchange platform and business. Frank is an international expert in data collaboration and has advised Australian State and Federal Government departments, multiple banks and insurers on data collaboration with the appropriate data security and governance techniques applied.

VANTEUM | galois | inpher

Dr. David Archer and Dr. Alex Malozemoff are Principal Investigators at Galois, Inc., a US-based cyber-security firm. Dr. Archer is a member of the United Nations Privacy Preserving Technology Team and lead author of that team's recent UN report on privacy and data sharing technologies. Dr. Archer also consults with the White House Office and select members of US Congress on privacy-preserving data-sharing technologies. Together, Dr. Malozemoff and Dr. Archer are Principal Investigators in privacy and cryptographic techniques for the US Department of Homeland Security, DARPA, and IARPA.

Sunny Seon Kang is Sr. Privacy Counsel and Head of Policy at Inpher, a US-based privacy-enhancing cryptography company with the conviction that encryption and privacy are foundational to the future of computing and commerce. Inpher applies years of academic research on Fully Homomorphic Encryption ("FHE") and secure Multi-Party Computation ("MPC") into commercially-ready applications that financial institutions are using in production today. Sunny leads Inpher's legal and public policy department and advocates for data protection by design, global privacy, and algorithmic accountability.

What we are seeing around the world

Through our experience working across the innovation ecosystem in Australia and also internationally, we have seen significant differences in how technology innovation is approached, supported and prioritised by Governments around the world.

As it is well known, Australia is abundant in natural resources and whilst it is understandable that Australia's major exports are currently these natural resources, this is not a sustainable export strategy into the future. We owe it to future generations to develop a far more mature innovation ecosystem that puts the development of technology including Fintech and Regtech at the core of our export strategy thus making Australia more globally competitive and to secure our economic prosperity.

There have been a number of recent reports calling out Australia's opportunity to use technology as both a source of economic prosperity through its use in Australia but also a key export. This includes the AlphaBeta report commissioned by CSIRO and Data61 where it is highlighted that

Digital technology could contribute up to $207BN in annual GDP if we were to catch up to our peer countries.[6]

The research conducted by the Harvard Kennedy Economic complexity[7] study on countries around the world as well has also called out such an opportunity for Australia and both have highlighted that “pragmatic, partnership-based approach[es] to policy reform will help Australia realise tech sector opportunities” alongside concrete recommendations on how Australia should further develop intellectual property, human capital, and focus on digital technology including Fintech and Regtech as key exports.

If Australia is to become truly competitive on a global stage in the areas of digital technology, artificial intelligence (AI), cybersecurity, and Fintech/Regtech as per some of the objectives set out by this inquiry, there are some fundamental shifts that need to be made in how we, as a country, prioritise the development of technology as a key export and thus organise the priorities and activities of government departments to support this.

In Ireland, for example, financial services and technology are key export themes under the nation’s “Innovation 2020” strategy and have been prioritised throughout the various government departments accordingly. As part of this national strategy, Ireland has also focused on the commercialisation of science and technology as a key theme for the financial prosperity of the country.

The introduction of the National IP Protocol in 2016 with further amendments in May of 2019 [8] provide for a simplified set of standards for research collaborations between the public and private sectors to make it even easier for a) research to be guided towards solving problems in industry and b) for this research to be turned into technology and used in the export market. Such a model contrasts sharply with a) the difficulty of commercialisation from an Australian University or other publicly funded research institute and b) the complexity of navigating intellectual property issues of such research collaborations between these institutions and private sector organisations.

These early-stage technology commercialisation efforts are then further supported through a suite of generous grants funding programs and an advanced equity investment program run by the Enterprise Ireland who have deployed over Euro1.32BN worth of equity capital since inception and who invested in 82 new early stage businesses in 2018 alone[9]. This makes them the third largest seed-stage investor in Europe (by deal flow). Enterprise Ireland also assist the early stage venture with additional capital raising from the private market at seed stage and in subsequent funding rounds.

In addition to the support given to the early stages of a technology company’s life, the Irish government also supports the international growth of such Irish Fintech and Regtech companies through their international network of Enterprise Ireland offices.

Singapore, through the work of AStar, Enterprise Singapore (ESG), and the Monetary Authority of Singapore (MAS) also focus on being regionally and globally competitive through the development of technology, financial services, Regtech and Fintech as key exports.

---

[6] Alphabeta report on Australia’s Digital Dividend
https://www.alphabeta.com/wp-content/uploads/2019/09/australias-digital-dividend-final.pdf

[7] Harvard Kennedy Atlas of Economic Complexity
http://atlas.cid.harvard.edu/

[8] Ireland’s National IP Protocol
https://www.knowledgetransferireland.com/Reports-Publications/Ireland-s-National-IP-Protocol-2019-.pdf

[9] Enterprise Ireland Seed and Veture Capital report 2018
https://www.enterprise-ireland.com/en/News/PressReleases/2019-Press-Releases/Enterprise-Ireland-publishes-Seed-and-Venture-Capital-Report-2018.html

The above international exemplars are consistent with other submissions to the inquiry including that of Regtech Australia[10] and public statements of Fintech Australia.

Unlocking value through data collaboration

Globally, we see an accelerating trend towards both private and public sector organisations collaborating to share data and unlock greater potential than the data any single organisation can access. Areas of such collaboration include the identification and prevention of tax fraud through network analysis of data held across multiple entities;monitoring and detection of money laundering across multiple banks; and identification of duplicate insurance claims across multiple insurers.

Furthermore, the use of sensitive data from otherwise segregated sources to achieve valuable public outcomes and inform evidence-based policy is increasingly important worldwide. In the United States, for example, juvenile justice laws permit data-sharing in search of improved juvenile justice and child welfare outcomes. In Estonia, statute allows for inter-agency data sharing for the purpose of detecting tax fraud.

One cautionary learning from such applications of data sharing is that extra steps must be taken to protect the privacy of citizens and their personal information. The common approach to sharing data among institutions is by transferring it from provider institutions (those that originally collect and hold the data) to consumer institutions (those that wish to use the data). When data is shared among multiple organizations in this way without additional protective measures, the *threat surface* of that data is increased. More organisations holding data means more potential for insider threats, external hacks, and intentional or unintentional misuse of that data. Spectacular failures of such protocols abound in the commercial and Government world, such as the “OPM Breach” of 2014 in the US. Unfortunately, the recent Australian Department of Health Data matching bill has called for this same approach to data sharing, putting the privacy of all citizens in Australia at risk. The significance of this issue cannot be understated as a) the Bill unintentionally prescribed the use of unencrypted data for data matching and for an out of date model of physical data exchange and b) the Bill passed both the lower house and Senate without any form of robust debate on cybersecurity and data privacy. This apparently highlights the lack of awareness of such issues in both the administrative government and in Australia’s Parliament.

Traditional approaches in data anonymisation have been proven outdated and ineffective in cryptographic and privacy analytics literature. For example, data de-identification has repeatedly been shown ineffective and subject to *re-identification attacks.* More importantly, de-identification effectiveness is known to be *undecidable* -- that is, there is no conclusive scientific basis for analyzing whether a de-identification approach is secure against attack. Another popular approach -- relying on the cyber security best practices of data sharers -- is also indefensible.

Modern network security practice begins with the assumption that all systems and networks are compromised, exposing all non-encrypted data. Shared data that brings together sensitive attributes from multiple data collection sources is a uniquely tempting target for the growing and highly profitable industry of cyber theft. PPPs provide alternatives that protect shared data without relying on de-identification or standard cyber security practices. These techniques include secure multi-party computation (data transforms into random auxiliary numbers that are deleted after each compute and cannot be pieced together to identify personal information), homomorphic encryption (encryption in-use, in addition to encryption at-rest and in-transit), zero knowledge proofs, and private set intersection that allow computation on data while it remains encrypted. Inpher has championed for the application of MPC and homomorphic encryption in financial services, consumer protection, improved AI modelling, and efficient enforcement to regulators and stakeholders in a global scale. Privacy-enhancing cryptography not only unlocks commercial

[10] Regtech Australia submission to Fintech and Regtech Senate inquiry https://www.aph.gov.au/DocumentStore.ashx?id=cc5caa48-cc7b-43bf-95f4-7f6df4199f6e&subId=674754

value; these techniques herald immeasurable public benefits by protecting the collective interest of privacy while facilitating valuable data-driven insights.

Moreover, there are secure hardware-enabled enclaves such as Intel Corporation's Software Guard eXtensions (SGX) that cryptographically protect data from access by other users on computer systems regardless of their credentials or authority; and differential privacy, which mathematically assures that statistical analysis results cannot be "reverse-engineered" to reveal source data. The value of such techniques have explicitly been called out by Dr. Ian Opperman, the NSW Chief Data Scientist in the Australian Computer Societies' Data Sharing taskforce.[11]

These techniques, combined with best practices in cryptography and cybersecurity, assure three key goals:

1. Data is shared among institutions only in encrypted form, so that it remains protected in transit, at rest, and during computation;
2. Results of computation on such data cannot be used to reveal that data; and
3. Utility of such data is not diminished or prevented by those privacy protocols.

It is probably no wonder that notable international organisations such as the World Economic Forum ("WEF"),[12] United Nations ("UN"),[13] Organisation for Economic Co-operation and Development ("OECD"),[14] and European Union Agency for Cybersecurity ("ENISA")[15] have all promoted the implementation of PPPs to minimise risks to privacy and data protection.

Applications in Regtech and Fintech

Privacy Preserving Protocols have significant and unique relevance in Regtech and Fintech settings to enable secure data collaborations that:

a. support innovation and competition

b. support systemic oversight and

c. further enhance decision making in Financial Services and Government settings

without compromising on security or the privacy of individuals.

---

[11] Australian Computer Society Privacy Preserving Data Sharing Frameworks Report https://www.acs.org.au/content/dam/acs/acs-publications/ACS%20Directed%20Ideation%20Report%20Aug%202019.pdf

[12] World Economic Forum, *The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value* (Sep. 12, 2019), https://www.weforum.org/whitepapers/the-next-generation-of-data-sharing-in-financial-services-using-privacy-enhancing-techniques-to-unlock-new-value

[13] United Nations, *UN Handbook on Privacy-Preserving Computation Techniques*, http://publications.officialstatistics.org/handbooks/privacy-preserving-techniques-handbook/UN%20Handbook%20for%20Privacy-Preserving%20Techniques.pdf

[14] OECD, *Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*: "The Joint Proposal also incorporates various recent data protection measures, including information management strategies, employee training, and appointment of individuals who are responsible for an organization's data protection practices, codes of practice, audits, privacy enhancing technologies, and privacy impact assessments." https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[15] European Union Agency for Cybersecurity (ENISA), *Privacy Enhancing Technologies 'Time to Adopt PETs'*, https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies

Domestic and International examples:

- The **Financial Conduct Authority** (FCA), a financial regulator in the UK, organized a week-long global anti-money laundering and financial crime hackathon in July 2019. A total of 10 teams participated, consisting of multiple companies and organizations, mainly from the tech and financial industries. These teams developed multiple solutions utilising secure computation technologies to enable banks to collaborate without sharing private customer data, while still allowing them to draw important insights. A team led by Microsoft developed a solution based on homomorphic encryption, a new encryption technology that allows computation to be done directly on encrypted data. They demonstrated how banks can issue encrypted queries to each other in customer onboarding scenarios to detect money mules. Microsoft has recently made significant investments in homomorphic encryption by creating and releasing open source tools, and driving a standardisation effort[16] for this technology.

- **Medicare claims fraud:** Recently, Vanteum and Galois outlined a way to leverage privacy preserving technology and methods to address up to $AUD600m of annual fraudulent medicare claims from data that currently resides in multiple Government Departments in a manner that both protects the privacy of citizens, the security of the data and involves no unencrypted data needing to leave any of the respective Government Departments. In addition to the above benefits, it would have addressed the concerns outlined in the Privacy Impact Assessments requested by Government and the concerns raised by the Australian Medical Association (AMA), the RACGP and NSW Civil LIberties on the “lack of sufficient privacy safeguards”. This is further demonstration of the power of Privacy Preserving Protocols to deliver social good whilst simultaneously enhancing and protecting the privacy of citizens.

- It should be noted that this same model to identify fraud and anomalies across multiple datasets is equally relevant to other Government Departments such as:

    - **The Australian Tax Office (ATO)** in the identification of possible cases of tax fraud - for example by analysing companies’ purchase and sales invoices while maintaining the data confidentiality of those transactions

    - **Australian Investments and Securities Commission (ASIC)**:
        - Prevent insider trading by sharing patterns and insights from trade data across institutions without sharing the underlying trade data itself.
        - Preventing bid rigging by replacing intermediaries with autonomous, transparent and incorruptible algorithms based on Privacy Preserving Protocols that perform the same service.

- **Insurance fraud:** Broadly speaking, the cost of fraud in the Insurance industry is shared between customers (who pay higher insurance premiums than would otherwise be needed to insure the actual risk) and financial institutions (which make payments on fraudulent claims that eat into their loss ratio, and thus ultimately their profitability).

  There are a number of possible opportunities for insurers to share data in order to reduce fraud, using car registration, claims, telematics, insured assets and customer data, as well as other unstructured data such as medical reports. This would allow institutions to realise two benefits:
    - An increased scale of shared data, leading to improved predictions and analysis. For example, an increased scale of claims data, telematics data

[16] Homomorphic Encryption standardisation body
https://HomomorphicEncryption.org

and other unstructured data would allow institutions to better identify patterns that suggest fraudulent claims.

- The identification of duplicate claims ("double dips"), filed against the same assets or the same incident across multiple insurers. However, much of this data is sensitive for insurers as their claims data is usually their most valuable. This is also accompanied by significant privacy concerns. Customers would not want their private information such as their registration data, claims data, personal information and other data such as medical reports being shared with third parties. Insurers themselves would be wary of sharing such information with their competitors, since it could be misused to deduce underwriting and pricing strategies, and other sensitive, competitive information. Through the application of PPPs it is possible for insurers to realise the benefits of data sharing as outlined above without the need to disclose or exchange unencrypted data. This protects the security and commercial sensitivity of the data, the privacy of individuals and unlocks significant value for insurers, the customer and the economy.

The development and application of these capabilities in and across, government, financial services and regulators has a significant opportunity to generate billions of dollars for the Australian economy, establish Australia as a leader in this field and create an environment where the protection of citizen data is never compromised.

Furthermore, there is an opportunity for Australia to leverage the capability built in this area as an export for the $127BN emerging global Regtech sector and differentiate our nation's capabilities on the protection of citizen data and the privacy of individuals.

Recommendations

- Organise specific trade missions for Senate committee representatives to both Ireland and Singapore to learn more about how these two countries and ecosystems operate and are designed to foster and support early-stage technology (including Fintech and Regtech) and Financial Services as key exports for their respective economies.

- Creation of a data privacy sub committee, which will:
    - Align with state and federal data privacy agencies to help streamline privacy requirements for technology companies.
    - Review and assess global best practice for data privacy.
    - Evaluate the potential of new technologies like the cryptography found in PPP
    - Create guidelines for technology companies to adopt data privacy best practice from the start.

- Appoint of Vanteum Chief Executive Officer, Alistair Muir to Senate Fintech Advisory Group and data privacy sub-committee.

- Creation of a working group to actively assess the use of Privacy Preserving Protocols in the context of FinTech & RegTech
    - Including the creation of a framework for the assessment of applicable technologies and methods for Government and Regulator driven data shares to enable greater collaboration whilst simultaneously protecting the security of data and the privacy of citizens.

- Education of Government Departments on the benefits of PPP:
    - when conducting inter-departmental data shares
    - when drafting new legislation.

- The Business Innovation fund remit should be expanded so that it supports earlier stage businesses at “seed” stage rather than that prescribed by the current scope of the fund that requires businesses have a minimum of $2 million annual revenue. This is consistent with the submission of Regtech Australia. A successful international example is that of Enterprise Ireland’s investment in High Potential Startups (HPSU) at seed stage. The criteria used by Enterprise Ireland is that the venture must have the potential to generate a minimum of E1 million within 3 years and is more consistent with an early stage venture capital model. [17]

[17] Enterprise Ireland High Potential Startup investment criteria
https://www.enterprise-ireland.com/en/Start-a-Business-in-Ireland/Do-I-qualify-as-a-HPSU-/

Conclusion

There is a significant opportunity for Australia to leverage Privacy Preserving Protocols to unlock value across Regtech and Financial Services by enabling secure data collaborations that:

A. Support innovation and competition
B. Support systemic oversight and
C. Further enhance decision making in Financial Services and Government settings

In addition to the application of these technologies in the domestic market, which could potentially unlock billions in value, there is an opportunity for Australia to leverage the capability built in this area as a technology export in a similar manner to countries such as Ireland and Singapore for the $127BN emerging global Regtech sector.

The key differentiator being that the security of citizens data and the privacy of individuals are never compromised.

We would welcome any requests for clarification or to provide more information to the Senate inquiry and its stakeholders on the techniques and technologies outlined in this submission.

Our contact details:

Vanteum:
Alistair Muir, Chief Executive Officer

Galois, Inc.
Dr. David Archer, Principal Investigator

Dr. Alex Malozemoff, Principal Investigator

Inpher:
Sunny Kang,
Sr. Privacy Counsel and Head of Policy

VANTEUM galois inpher