

## Introduction

We would like to thank the Department of Health for consulting with the Australian public on the significant set of legislative changes, their impact on the privacy of individuals; and for structuring a consultation that welcomes comments on all aspects of the proposed changes.

We commend the direction and intent to reduce claims fraud that currently costs the Australian Taxpayer hundreds of millions of dollars by leveraging the information that is currently held by various Government departments.

Furthermore, the use of sensitive data from multiple otherwise separate sources to achieve valuable public outcomes and inform evidence-based policy is increasingly important worldwide. In the U.S.A. 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 key learning from such data sharing settings is that extra steps must be taken to protect the privacy of citizens and their personal information. Spectacular failures of such protection abound in the commercial and Government world, such as the “OPM Breach” of 2014 in the US.

As a Global consortium with significant experience in data sharing and the protection of personal data, we are concerned that the proposed legislation does not address the protection of citizen personal information adequately, and does not take into consideration more contemporary models and technology that other governments around the world are utilizing. In particular, the privacy mechanisms provided in Section 132F(2) seem insufficient and incomplete.

As a consequence, we feel that the proposed legislation puts the identities of every Australian at considerable risk. However, this risk can be mitigated through appropriate design and implementation of privacy-preserving data sharing capabilities that are based on more contemporary methods.

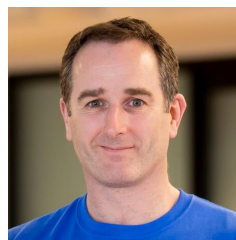
## About us

Vanteum and Galois are a global consortium comprised of Data governance and data security experts who have repeatedly and successfully addressed and solved problems at the intersection of privacy and public good. Our experience spans state and federal government in domains of Defence, Intelligence, Health, and Financial Services.

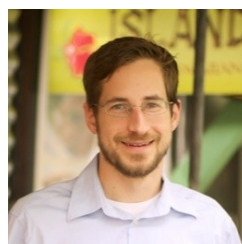
### Specific people involved:



**Alistair Muir is the CEO 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 on the use of data to solve industry problems.



**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.



**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.

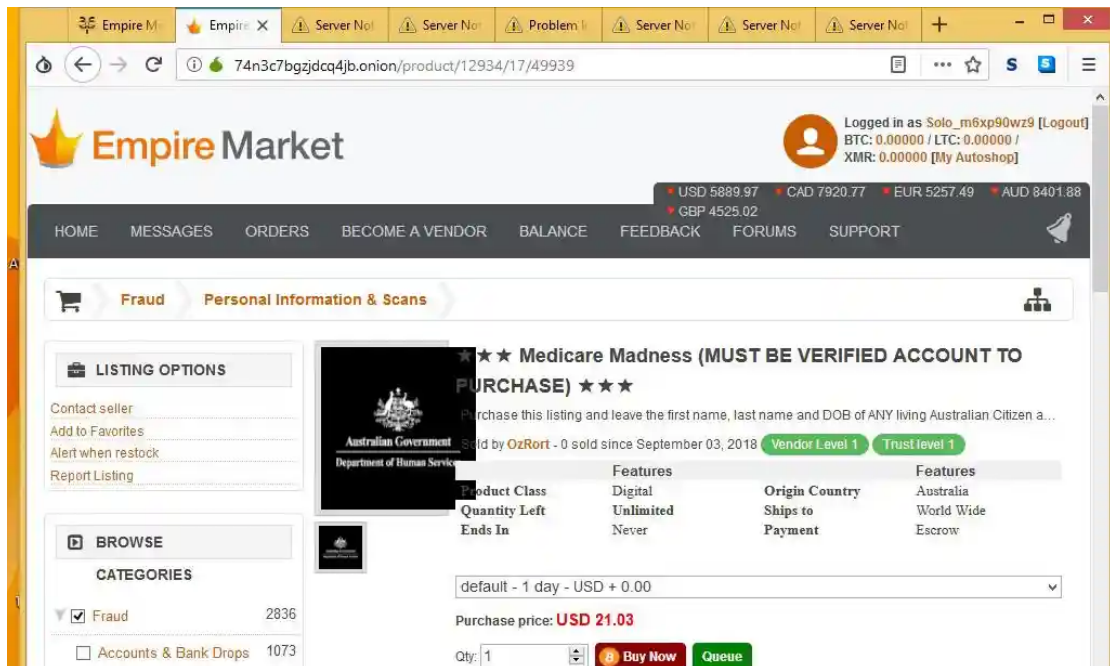
## What we are seeing around the world

In the old but still common paradigm of data sharing, institutions share by transferring data from provider institutions to other institutions that wish to use the data. When data is transferred from multiple institutions to a central repository (such as that described in the model outlined in this draft legislation), the resulting, richer dataset is a highly tempting target for theft and misuse.

While there have been many attempts to improve security protections for such data, for example by applying data de-identification prior to sharing or substituting in synthetically created data, these techniques often fail to protect data while at the same time reducing their utility. Thus such data are attractive as a target of the growing and profitable industry of cyber theft that affects all databases worldwide.

One relevant example of cyber theft is the continuing operation of the dark-web business known as Medicare Madness, which offers Medicare card details of Australian citizens for sale at roughly \$AU31 a piece, as shown in the screen-shot below.

The breach that gave rise to this business, and the continued inability to shut it down after a year of effort, led one political spokeswoman to say of the Government, "It's a reminder of [a] shocking record on privacy and cyber security." Such comments are unhelpful, but are indicative of a growing lack of trust in the ability to protect shared data, which in turn makes organisations unwilling to share such data with their counterparts.



The screenshot shows a web browser window displaying the Empire Market website. The page is for a listing titled "Medicare Madness (MUST BE VERIFIED ACCOUNT TO PURCHASE)". The listing is for "Australian Government Department of Human Services" and is sold by "OzRort". The purchase price is listed as USD 21.03. The listing includes details such as "Product Class: Digital", "Quantity Left: Unlimited", "Ends In: Never", "Origin Country: Australia", "Ships to: World Wide", and "Payment: Escrow". The page also shows a navigation menu with options like HOME, MESSAGES, ORDERS, and a sidebar with "LISTING OPTIONS" and "BROWSE" sections.

In addition to the above example, there are many noteworthy breaches across the world that demonstrate the inability of organisations to protect data. Examples include:

- Serious security incidents in the UK where the data of 150,000 NHS “opt-out” patients were inadvertently shared with third parties.
- The “OPM breach” in March 2014 in the US, where personal data of 21.5M individuals, including fingerprints, financial accounts, and credit records, were stolen.
- Commercial breaches such as at the Equifax credit reporting service, where 146M credit records were stolen in 2017; and the Marriott/Starwood breach where the records of 500M hotel guests were stolen in 2018. Such breaches also include events such as the Ashley Madison breach that resulted in suicides by subscribers.

Because such breaches continue to increase dramatically every year, it is no wonder that we see rising adoption in the private sector and Government organisations of the technologies of *Privacy Preserving Protocols* to protect shared data from theft/misuse. Such protocols enable

the desired benefits of data collaboration without the need to disclose and exchange sensitive data “in the clear”.

Privacy preserving protocols include techniques such as *secure multi-party computation*, *homomorphic encryption*, *zero knowledge proofs*, and *private set intersection* that allow computation on data while it remains encrypted; secure hardware-enabled enclaves such as Intel Corporation’s *Software Guard eXtensions* (SGX) that can be used to protect data from access on many versions of Intel processors; and *differential privacy*, which mathematically assures that statistical analysis results cannot be “reverse-engineered” to reveal source data.

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

1. Data is shared among institutions only in encrypted form;
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.

## Key concerns with the privacy provisions of the legislative package

Without a more comprehensive set of provisions for privacy assurance, every Australian citizen will have their privacy put at serious risk in order to achieve the public good that the Bill aims to achieve. Our guiding principle, in contrast, is that citizens’ privacy and public good need not be mutually exclusive.

Whilst supportive of the use of data collaboration to increase compliance, we’d like to again highlight that the same intended benefits can be achieved without moving, centralising or needing the data to be in any other form but encrypted. These risks have already been highlighted in the Privacy Impact Assessment prepared by King and Wood Mallesons (K&WM) and Galexia as part of the consultation and the recommendations posed under sections APP3 (Collection of solicited personal information), APP11 (Security) and Section 18 Privacy Governance <sup>1</sup> agree with ours.

Additionally, **Section 132F(2)** of the draft Data matching bill, and more broadly the rest of the Bill, prescribe protections of individual privacy that are based on old and flawed paradigms. We suggest the new legislation must be drafted in a particular way that address the challenges of the;

- Protection against malicious exfiltration
- Protection against insider threats
- Protection against accidental disclosure
- Creation of a sharing control system that limits the availability of information on a need-to-know basis as well as a well-defined access expiry process

### Removal of the unintentional prescription of movement, centralisation or supply of unencrypted data from the Bill.

The current draft uses phrases such as “provide to” or “obtain by” and these could be interpreted as necessitating movement of data and/or exclusion of distributed analytics. For example, in Schedule 1: Amendments, Part 1: Data-matching, Section: 132B, “information that has been provided to the Chief Executive Medicare in accordance with any of the following Acts”.

Similarly, the use of the word “disclose” may bias the interpretation that an organisation must provide or allow for data to be supplied or used unencrypted, e.g., “a private health insurer may disclose to the Chief Executive Medicare”.

---

<sup>1</sup> Department of Health Data Matching PIA – Fraud Detection and Compliance Activities (September 2019) by King & Wood Mallesons/Galexia

We suggest that a greater familiarisation with contemporary global data collaboration best practices is required to prevent a bill being drafted that is not based on outdated models and the prescription of out of date technology to achieve the intended means.

### **Update of the security and data matching frameworks used in the legislation.**

Again, while very supportive of the use of standard technology security frameworks within the implementation, the ones suggested in the consultation paper are critically out-of-date<sup>2</sup>. For example, the core technical guideline recommended to be used, “Guidelines on data matching in Australian Government administration”, is from June 2014, over 5 years old or a generation ago in security and privacy technologies terms. Some frameworks suggested are over 10 years old. Security technology and approaches, in particular around privacy, have seen paradigm shifts since then.

In particular, the “Guidelines on data matching in Australian Government administration” has a strong emphasis on moving, storing and deleting data. Again, given the risks, we suggest that the implementation frameworks used should incorporate and strongly advocate the consideration of more current privacy preserving protocols.

With the application of modern techniques in the field of Privacy Preserving Protocols, it is both possible and proven that Government departments can safely get the benefits of data collaboration without the need to move nor disclose the data itself. This would also address the concerns raised in the Privacy Impact Assessment APP3, Recommendation 5, “Only collecting data fields that are necessary and using data verification” and reduces the security risks called out in recommendations 9 and 10 of the same PIA.

While a complete assessment of such damage is well beyond our scope here, we offer the following examples of lost privacy that can still occur under the provisions of the proposed Act:

- Leakage of Medicare data that has already occurred and is being sold on the dark web (as per example outlined above)
- Misuse of data both intentionally and accidentally
  - The intentional misuse by staff and 3rd parties cleared to view the raw data is a constant risk and one which can only be mitigated by the use of techniques provided by privacy preserving protocols.
  - The accidental misuse of data / human error is unfortunately a common occurrence globally and offers the same risk profile as intentional misuse. When certain privacy preserving protocols are used the raw data is never decrypted and therefore mitigates this risk.

## **Responses to specific stakeholder questions**

### **1. Do you have concerns about this legislation with regard to privacy protections, the Privacy Act 1988 or the role of the Australian Information Commissioner?**

We do have concerns regarding privacy protections. The draft legislation as written codifies the notion of explicit data sharing as a requirement. However, as we described above, such data sharing provides a single point-of-failure that is highly susceptible to cyber attacks, insider threats, and accidental disclosure. As a result, there is a long history of breaches in such sharing frameworks.

Unfortunately, the legislation does not address this concern. We believe that the legislation should directly address the need for *secure data collaboration* employing modern technical privacy protections, including the privacy preserving protocols we describe above. Directly addressing privacy assurance both protects Australian citizens’

<sup>2</sup> Consultation Guide: The Health Legislation Amendment (Data-matching) Bill 2019 and Associated Regulations

private information and fosters confidence in an expanded cohort of participants. In addition, inclusion of privacy protection provisions in the legislation would put it on a comparable footing with worldwide Government policies, corporate practices, and technology evaluations regarding privacy, such as these examples:

**Government Policies.** In Europe, the *General Data Protection Regulation* (GDPR) enforces strict privacy controls for its citizens, and the recent *California Consumer Privacy Act* (CCPA) brings similar protections to California residents. Several bills in the US have also been introduced that explicitly mandate the use of privacy preserving protocols due to privacy concerns. These include the *Student Right to Know Before You Go Act of 2017* and the *FORWARD Act of 2018*.

**Corporate Practices.** Within the commercial sector, many large corporations, including Google, Apple, and Cloudflare, are utilizing privacy preserving protocols both internally and externally. Google utilizes *private set intersection* in order to share advertisement placement information with advertisers in a secure fashion; Apple uses *differential privacy* to collect user information in a privacy preserving fashion; and Cloudflare utilizes privacy preserving protocols to enhance usability while limiting its ability to track users.

**Technology Evaluations.** Privacy preserving protocols have a long history of use in both Government run pilot studies alongside use within the private sector. In the US, the Bipartisan Policy Center recently reported results of a successful pilot that applied privacy preserving protocols to analytics for evidence-based policymaking at the County level of government. In that study, databases from five diverse County organizations were combined to analyze resource allocation for public services, while cryptographically protecting all data about individuals used in the analysis.

Also in the US, the Boston Women's Workforce Coalition has established an ongoing pilot program that analyzes salary equity among participating companies in the Boston area without revealing any salary information. Other pilots are in progress or under consideration for multiple US states to analyze education data for purposes such as identifying school and school district performance trends without revealing any individual student data. In the UK, the Financial Conduct Authority (FCA), is piloting several applications of Privacy Preserving Protocols to enable both private and public sector organisations to work together through data collaboration to tackle cases of money laundering without requiring either party to disclose their data.

All of these examples demonstrate both the relevance and applicability of such technology within Government and the private sector.

In addition to stipulating technical privacy protections, we feel that the legislation should include provisions to sponsor the kind of privacy technology evaluations cited above. Such provisions are included in the US legislation described above, and can stimulate both Government leadership in technology adoption, and academic and industry development of relevant technologies.

2. *Are there any additional agencies and entities that should be listed for potential disclosure of MBS and/or PBS information, or notification of compliance outcomes for public interest reasons?*
3. **Are there any other data sources that would be appropriate to match with MBS and/or PBS data for Medicare compliance purposes?**
  - If the legislation was to adopt the use of Privacy Preserving Protocols we speculate given what we have seen globally that the increased level of privacy awarded to the data would significantly increase the level of participation.
4. *Are there any additional safety and quality concerns in the health system that could be addressed through access to other data?*
5. *Should there be any other compliance purposes that should be permitted under the proposed legislation?*



**6. Are there adequate transparency and accountability mechanisms built in to the framework?**

- We recommend the Department of Health consider using privacy preserving protocols to encrypt the datasets in each of the participants databases and consider performing the analysis in a federated or distributed manner to decrease both the risk and requirement for increased governance of a centralised database of such sensitive data and further fosters:
  - i. **Transparency:** by maintaining a decentralised system using Privacy Preserving Protocols, it allows control of the data and its use to be shared and maintained by the control by both data custodians and Health Dept. There is no central honeypot and usage of encrypted data can be tracked and governed at source as well as by Health Dept.
  - ii. **Accountability:** Again, the distributed nature of the proposition (data, analytics and governance) and proper control of encryption keys allow for increased accountability and control by whole ecosystem of data custodians while not impacting results/benefits.

## Conclusion

We commend the intent of the draft Act to leverage the data of multiple participants to cut down on Fraud that costs the taxpayer hundreds of millions of dollars. The legislative package as it currently stands, however, is based on outdated technology and practices which require the data to be “moved” and analysed in a central location.

Without a more comprehensive set of provisions for privacy assurance, every Australian citizen will have their privacy put at serious risk in order to achieve the public good that this Bill aims to achieve. Our guiding principle, in contrast, is that citizens’ privacy and public good need not be mutually exclusive.

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

**Our contact details:**

**Vanteum:**

Alistair Muir, Chief Executive Officer  
T: +61 457 540 224  
E: alistair@vanteum.io

**Galois, Inc.**

Dr. David Archer, Principal Investigator  
E: dwa@galois.com

Dr. Alex Malozemoff, Principal Investigator  
E: amaloz@galois.com