September 2017

Data Sharing Frameworks

Technical White Paper

Thanks to the following organisations

Australian Government

Department of the
Prime Minister and Cabinet

Australian Government

Australian Institute of
Health and Welfare

Foreword

You only have to look at the smartphone in your hand to realise how entrenched technology has become in our lives. And all technology — no matter how large or small — reads, processes, and creates data. Indeed, data underpins and is the lifeblood of every technical innovation we use today.

As we look to a future increasingly driven by the potential of machine learning and artificial intelligence, the volume and value of this data will only increase.

Naturally, not all data is created equal. Some data, particularly that containing personal information, has a higher value and at the same time comes with an element of trust — that this information will be protected by the business or Government entity holding it.

Indeed, privacy is a critical component of trust for any business or Government service. Yet opening up this data to be shared greatly increases the potential for better delivery of products and services, or for entirely new products and services to be created.

One of the key challenges, then, is how can we create an environment for the sharing of data while retaining and protecting individual privacy in cases where personally identifiable information is present.

It is not, by and large, a simple problem to solve. It crosses not just technical boundaries, but social and ethical ones as well. There is as much a need for education around the value of data as there is for the potential data offers when shared in the right environment with the right controls.

This white paper, sponsored by the ACS and led by Dr Ian Oppermann, NSW's Chief Data Scientist and CEO of the NSW Data Analytics Centre, is a first step in opening and driving the conversation — and on the potential and challenges of data sharing — by starting to define a data sharing framework.

It's not an easy task, and there's more work to be done, but it is my hope that by releasing this white paper to a wider audience we can galvanise discussion and further explore how we can create reliable, secure, shared data services for business and Government that will benefit all Australians.

The Hon Victor Dominello MP
NSW Minister for Finance,
Services and Property

Executive Summary

Future smart services for homes, factories, cities, and governments rely on sharing of large volumes of often personal data between individuals and organisations, or between individuals and governments. The benefit is the ability to create locally optimised or individually personalised services based on personal preference, as well as an understanding of the wider network of users and providers.

Data sharing comes with a wide range of challenges broadly categorised as: data format and meaning; legal obligations; privacy; data security; and concerns about unintended consequences of data sharing. This creates the need to develop sharing frameworks which address technical challenges, embed regulatory frameworks, and anticipate and address concerns as to fairness and equity of outcomes in order to maintain trust of consumers and citizens.

A Data Taskforce has been created to address the overarching challenge of developing ethical and privacy-preserving frameworks which support automated data sharing to facilitate smart services creation and deployment. This framework will seek to address technical, regulatory, and authorising frameworks. The intention is to identify, adopt, adapt, or develop frameworks for data governance, privacy protection, and practical data sharing which facilitates smart service creation and cross jurisdictional data sharing between governments. The approach is to identify best practice where it is known to exist; consider existing models in an Australian privacy and cultural context; or identify 'whitespace' opportunities to develop frameworks for Australia.

Dr Ian Opermann
CEO and Chief Data Scientist, NSW Data Analytics Centre
ACS Vice President - Technical Advisory Board

A summary of challenges identified for continued investigation are:

CHALLENGE 1

Defining the characteristics of data sets which meaningfully span the spectrum covering: non-personal data, highly aggregated (or perturbed) personal data sets, lightly aggregated (or perturbed) personal data sets, and data sets which contain personally identifiable information (excluding health information).

CHALLENGE 2

Characterisation of 'smart service' types – and the associated limitations and obligations of service providers – based on the data sets used to create them.

CHALLENGE 3

Regulatory and trust clarification – developing a clear, concise statement of the legal, policy and ethical frameworks which enable data sharing for smart services types based on the underlying data sets used.

CHALLENGE 4

Identification of Personally Identifiable Information (PII) – developing an unambiguous test for the presence of personally identifiable information within a set of data sets.

CHALLENGE 5

Development of trusted data sharing frameworks – many restrictions on data sharing are due to concerns about appropriate use and interpretation of data, concerns about unintended consequences of sharing data, concerns about accidental release of sensitive data, and concerns about adherence to legislation. Frameworks for trusted data sharing would help address these challenges.

Contents

01

Introduction

Future smart services for homes, factories, cities, and governments rely on sharing large volumes of potentially personal data between individuals and organisations, or between individuals and governments. The benefit is the ability to create locally optimised or personalised services, as well as developing an understanding of the wider network of users and providers.

Data sharing comes with a wide range of challenges broadly categorised as: data format and meaning; legal obligations; privacy; data security; and concerns about unintended consequences of data sharing. This creates the need to develop sharing frameworks which address technical challenges, embed regulatory frameworks, and that anticipate and address personal or cultural concerns as to fairness and equity of outcomes in order to maintain trust of consumers and citizens.

The relationship between information and data creates a fundamental challenge which is at the heart of many of the issues of data sharing. In a closed system, there is a well-defined relationship between information (related to the likelihood of an event occurring) and the data needed to represent the information in that event. This relationship is very well understood from information theory and has been used for the last 70 years as the basis for all modern digital communications systems, from mobile telephony to digital television broadcasting and data encryption. The reverse process of identifying information events in data is not as well defined, but it is broadly true to say that data can carry high levels of information, and combining data sets can create even higher information events.

The practical reality is that data sharing does not occur in a vacuum. In almost any environment, data from other sources can be brought together with data which has been shared. This leads to the well-known 'linkage' or 'mosaic' challenge whereby aggregated data can be decomposed by linking with external data sets. The ability to increase either the value of a shared data set, or the level of personally identifying information within shared data sets, is limited only by the ability to link extraneous data to the sets which have been shared.

When data is shared, it enters an environment which has contextual information. Every human recipient of data interprets data with context. Each of us knows something of the world, of relationships, of individuals and of history. Similar to the linkage problem, the context of a shared data environment means the value of a shared data set, or the level of personal information, can be increased by individual context.

It is this complexity of human environments which makes the evaluation of the existence of personal information so challenging to assess. It also provides the basis for authorising or sharing networks, which describe who should get access to data under what circumstances. Trust also forms a very large part of the context in which data is shared with different levels of trust associated with different contexts, resulting in different levels of willingness to share data.

People also have social norms and personal values which will provide the basis of when and under what circumstances they are willing to share or pass on data. Willingness to share data is set within a cultural framework – with different norms for sharing data informed by regulation, social constructs, and personal values frameworks.

It is this complexity of human environments which makes the evaluation of the existence of personal information so challenging to assess. It also provides the basis for authorising or sharing networks, which describe who should get access to data under what circumstances. Throughout this document, we will refine an organisational framework which will be used to define the problem space, and help to identify areas for specific focus.

02

Data Taskforce

A Data Taskforce led by the Australian Computer Society (ACS), and the NSW Data Analytics Centre (DAC) has been created to address the overarching challenge of developing privacy-preserving frameworks which support automated data sharing to facilitate smart services creation and deployment. This framework will seek to address technical, regulatory, and authorising frameworks. The intention is to identify, adopt, adapt, or develop frameworks for data governance, privacy preservation, and practical data sharing which facilitates smart service creation and cross-jurisdictional data sharing between governments. The approach is to identify best practice where it is known to exist; consider existing models in an Australian privacy context; or identify 'whitespace' opportunities to develop frameworks for Australia.

The Taskforce has been meeting since June 2016, with representatives from ACS, the NSW DAC, Standards Australia, the office of the NSW Privacy Commissioner, the NSW Information Commissioner, the Federal Government's Digital Transformation Office (DTO), CSIRO, Data61, the Department of Prime Minister and Cabinet, the Australian Institute of Health and Wealthfare, SN-NT DataLink, Victorian Government, West Australian Government, Queensland Government, Gilbert and Tobin, the Communications Alliance, the Internet of Things Alliance, Objective, Telstra, IBM, Mastercard, and Microsoft. The Taskforce has subsequently met through to August 2017 to continue developing the privacy preserving frameworks. This technical white paper is the first significant output of the Taskforce.

2.1 GOALS OF THE TASKFORCE

The overarching goal is to support the development and deployment of smart services in an Australian context which is consistent with Australian privacy legislation.

This will be facilitated by:

- Developing frameworks which characterise sets of data based on the degree of personal information contained within them (nominally referred to as a 'Personal Information Factor')
- Developing frameworks which characterise 'smart service' types based on the data sets used to create them and the associated Personal Information Factor
- Developing trust frameworks which allow data to be shared, joined, and used in operational environments whilst preserving individual privacy
- Identifying ways of clarifying existing State and Commonwealth Privacy Acts through quantified descriptions of acceptable levels of risk in ways which are meaningful for modern data analytics.

2.2 FOCUS AREAS

The four focus areas for this Taskforce are: cross jurisdictional open data sharing, governance, privacy, and practical data sharing – as shown in Figure 1.

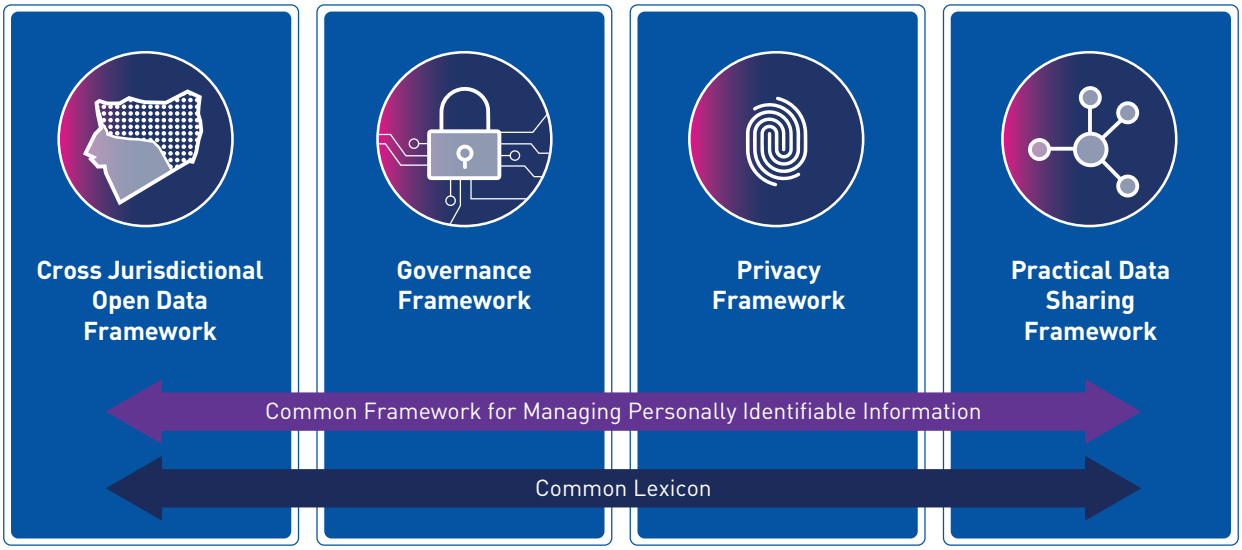


Figure 1. Focus areas of the Taskforce

A summary of challenges identified for continued investigation are:

CHALLENGE 1

Defining the characteristics of data sets which meaningfully span the spectrum covering: non-personal data, highly aggregated (or perturbed) personal data sets, lightly aggregated (or perturbed) personal data sets, and data sets which contain personally identifiable information (excluding health information).

CHALLENGE 2

Characterisation of 'smart service' types – and the associated limitations and obligations of service providers – based on the data sets used to create them.

CHALLENGE 3

Regulatory and trust clarification – developing a clear, concise statement of the legal, policy and ethical frameworks which enable data sharing for smart services types based on the underlying data sets used.

CHALLENGE 4

Identification of Personally Identifiable Information (PII) – developing an unambiguous test for the presence of personally identifiable information within a sets of data sets.

CHALLENGE 5

Development of trusted data sharing frameworks – many restrictions on data sharing are due to concerns about appropriate use and interpretation of data, concerns about unintended consequences of sharing data, concerns about accidental release of sensitive data, and concerns about adherence to legislation. Frameworks for trusted data sharing would help address these challenges.

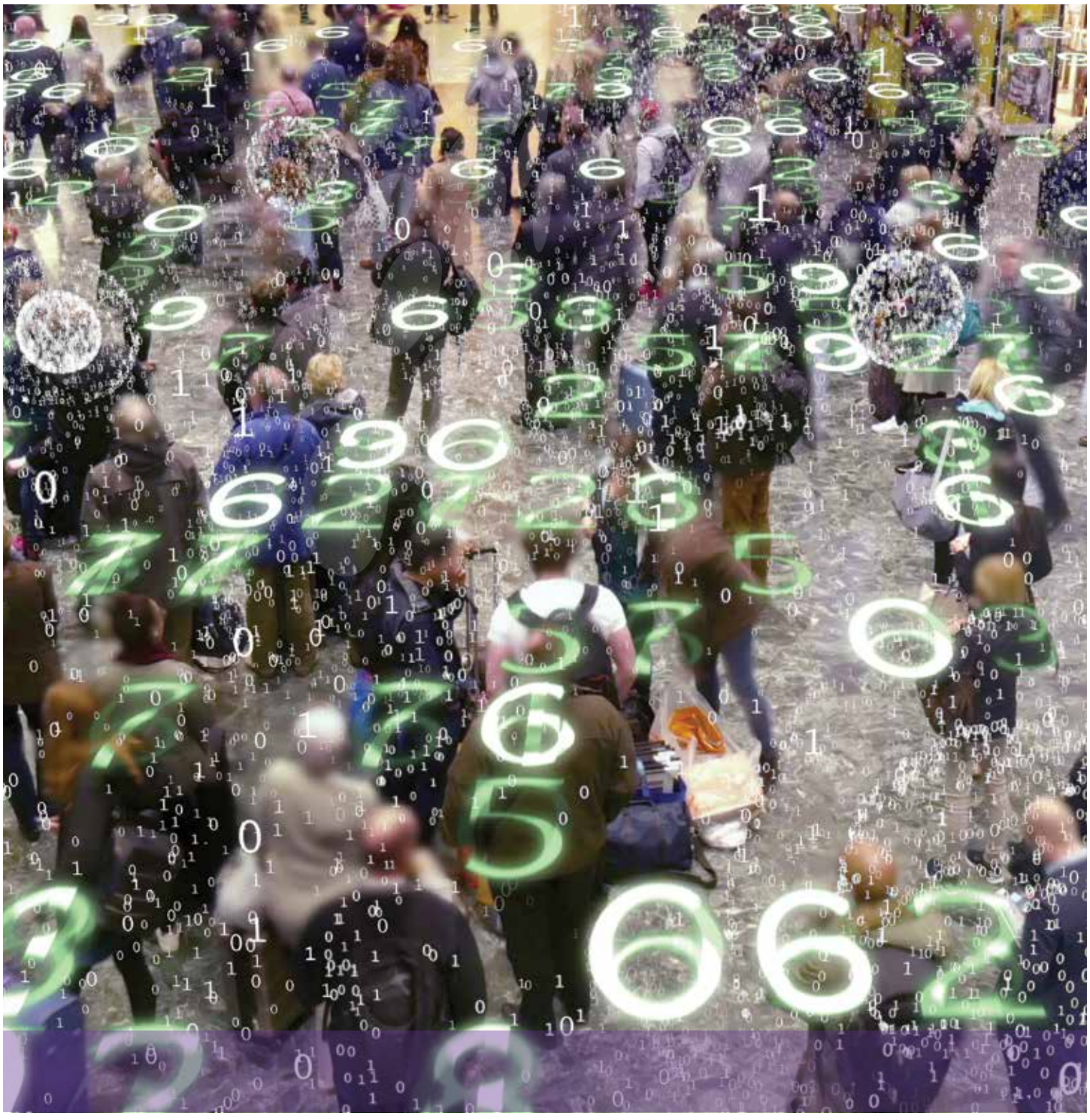
Data Availability and Use Inquiry

The Productivity Commission Data Availability and Use Inquiry Report released in March 2017 has investigated the benefits and costs of options for improving availability and increasing the productive use of data from the public and private sectors.

With significant range of recommendations and reforms identified to increase and improve data linking, availability and productive use, the Australian Government is currently preparing the response to the Inquiry recommendations through the Department for the Prime Minister and Cabinet.

The implementation of a new data sharing framework with meaningful engagement by the community was recognised as critically important by the Inquiry. The Inquiry also affirmed the importance that standards and that the development of data formats and definitions would be industry led, rather than undertaken by government.

03



Reframing the Conversation – Bits not Atoms

In his 1995 book *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*[1], Don Tapscott first presented the term 'Digital Economy'. Nicholas Negroponte subsequently used the metaphor of shifting from "processing atoms to processing bits" as a means of explaining the transition towards a digital economy and associated increasing reliance on products and services which are underpinned by data. The digital economy is now described by some economists as the sector of the economy associated with 'zero marginal cost intangible goods available on the internet'[2].

A fundamental shift in mindset is required when we consider the pervasive role, use and value of data in the digital economy, and in a digitally enabled society. Often discussions on the digital economy are framed as if digital products and services are simply the digital manifestation of physical goods, or of traditional services, which are exchanged bilaterally and effectively monopolised or extinguished on consumption.

There is a fundamental conceptual reframing required to understand the multiple uses and reuses of data which underpins the digital economy. Data can be the product itself, can be used to create the digital service, to understand the interaction with the digital service, to understand a wider set of relationships or even to predict a future state or need. The same data can then be used for further unrelated purposes creating additional value by third parties.

The legal, privacy and accounting frameworks which have been developed for dealing with assets and intellectual property also fall short when we consider a greatly expanded role of data, and what becomes possible when sophisticated data analytics are applied.

When the value of the service is created from the manipulation of data, questions often follow such as 'Who owns the data?' and 'Can I have access to all of my data?'. These are challenging questions to address as data does not exhibit the characteristics of a traditional asset (including software), of a traditional factor of production (land, labour, or capital), or even of intellectual property. The ability to effortlessly use, replicate and share data means it cannot be considered in the same way as a physical asset with an 'owner'. Rather, it is important to think of rights, roles, responsibilities, and limitations for those who access data in the various processes from collection, use, sharing and storage.

It is useful to focus on the services derived from data rather than the data itself. Reframing thinking in this way means the focus can be shifted to the impact from the use of data. Service creation, delivery and even consumption can then be described in terms of rights, responsibilities, restrictions, and obligations. The simplest of services may just be making data available.

3.1 WHAT IS DATA?

Data does not exist in any physical sense other than the manifestation in the medium used to represent it. The shape of an ink symbol on paper, the magnetic orientation of a 'bit' on a hard drive, or the phase of a radio frequency signal propagating through space all carry bits of data – but are not data in themselves.

1. D. Tapscott, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*, May 1997, McGraw-Hill
2. See for example L. Fournier, *Merchant Sharing, Towards a Zero Marginal Cost Economy*, May 2014. Available online https://arxiv.org/pdf/1405.2051.pdf (Accessed 6 August 2017)

Each mode of storing or carrying data can be used for a period of time before the data is moved to the next medium for further transmission, visualisation, copying, combination with other data, or for long-term storage.

In some economic frameworks, data is treated in a similar way to intellectual property or software. The World Intellectual Property Organization describes intellectual property as *"creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce"*[3] with no explicit reference to data. There is currently no Australian Accounting Standard that comprehensively addresses the accounting treatment of data or even of intellectual property.

IP Australia states that most relevant accounting standards include:

- AASB 138: Intangible Assets
- AASB 136: Impairment of Assets
- Accounting Interpretation 132: Intangible Assets Web Site Costs

IP Australia further states that many Australian companies do not recognise their acquired intellectual property, instead often including it on their financial statements as goodwill.

Data is unlike a brand in that it can be used in many different ways for many different applications. It is different to software in that it may have no inherent operational function. Data is different to goodwill in that it can be sold in discrete volumes to individual users. It is different to copyright in that it needs resources to capture, contain or transport it. Data is even different to community-generated intangible assets such as open source software in the sense that a company, such as Facebook, can exclusively own the collection of data created by many individuals.

Treating data as a durable capital good – one which does not quickly wear out that and that is used in the production of goods or services – also does not capture the unique nature of data. It is relatively easy to see how a licence for word processing software can be viewed as a durable capital good. For use of that software by an additional employee, an additional licence is required (it is discrete). Access to the software can reasonably be expected to make that employee more productive (it is like capital) and will do so for some years (it is durable).

Taking this view for data, however, dramatically underemphasises the role of very large, highly scalable software platforms which become the environment within which services are created for and by others. Ridesharing company Uber and the online game Minecraft are examples of massively scalable platforms which provide services to millions of users by processing large amounts of personal data.

The ability to scale output requires a small amount of the traditional factors of production: land, labour, and capital. Their most important input is arguably the data generated by the apps running on the devices of gamers, or the smart phones of ridesharing passengers and drivers around the globe. Uber's ability to scale their service output to new customers is only weakly dependent on the level of land, labour, and capital. Without user and driver generated data, their businesses would not function.

Framing data as intellectual property becomes increasingly inadequate when the data is not generated by the entity which uses it. In the case of social media companies such as LinkedIn, Twitter and Facebook, user-generated data is harnessed to create services. These services encourage creation of more user-generated data, and so more services. The value of the platform to the business is driven by ever more users freely contributing data, and less and less by the intellectual property in the underlying service creation. If users suddenly stopped providing data, the businesses would not function.

3. See http://www.wipo.int/about-ip/en/ (Accessed 6 August 2017)

3.2 THE RELATIONSHIP BETWEEN INFORMATION AND DATA

An information theoretic definition states that the amount of information associated with a given value being generated by a random process is inversely related to the probability of that value occurring. As an alternative description, the less likely a particular value is of occurring, the more information associated with the occurrence of that value. The number of information 'bits' is then the logarithm (base 2) of the inverse of this probability[4,5].

This approach to quantifying information has been used for more than 70 years to analyse the information associated with communications systems. In 1948, Claude Shannon published his landmark paper, *A Mathematical Theory of Communication* in the Bell Systems Technical Journal. Shannon showed how all recorded information could be quantified with precision and demonstrated that information media – ranging from telephone signals, text, radio waves or pictures – could be encoded as digital bits and transmitted at a known maximum rate over a channel.

The information theoretic model has been applied in ever expanding fields of information media which can be represented in data. The theoretical frameworks developed are however only strictly applicable when a data source is well defined and the communication channel can be accurately characterised.

The mapping of information to data is clearly understood and has underpinned much of the digital revolution experienced in modern times. Mapping in the reverse direction – from data to information – is an equally interesting process. The corollary might be: when data sets are combined to create a value, which has low probability of occurring, then there is information associated with the occurrence of that value. There is little mathematical study into this hypothesised corollary, however it intuitively seems reasonable that combining ,and for example visualising, sets of data sets allows an observer to identify events (values) which are unexpected (low probability).

The challenge is, when the observer is a human being, they bring a rich context to observation, including data sets explored, observation circumstances, motivation for observing, personal experience, personal judgement, and personal bias. The ability to generate values which are 'unexpected' becomes a far more complex challenge to address, as does the ability to quantify what is 'unexpected'. Nonetheless, additional data sets which are joined, and a change in observer context, may lead to a range of 'unexpected' results being observed.

4. See for example R. M. Gray, *Entropy and Information Theory*, Springer-Verlag, 2014. Available online http://ee.stanford.edu/~gray/it.pdf
5. Importantly, another fundamental of information theory states that additional processing of data will not create additional information beyond what is already present. This is an important consideration when considering the limits of analytical models.

04

Shared Data

Very often, 'shared data' is assumed to be that which is shared *directly* between individuals or organisations. A person may provide name, address, date of birth, height, or preference details in exchange for some service or benefit.

Data may be gathered about an individual or system in other means by:

- **Observation** – counting cars or pedestrians, observing behaviours, or the presence of a beard
- **Derivation** – combining several directly-shared or observed factors to produce a result with high certainty. A trivial example may be observing an individual with a beard and deriving the gender of that individual
- **Inference** (deduction) – combining several directly shared or observed factors to produce a result with moderate to high certainty, as popularised by the fictional detective Sherlock Holmes.

In all cases, personal information is involved. Other than the direct sharing example, there is no consent of the individual from whom the data is observed, derived, or inferred. The data is created by a third party through observation, applying external information (derived), and by applying logical processes and external information (inferred) to produce some new information.

4.1 A BASIC DATA SHARING FRAMEWORK

Once a data set has been created, a basic framework can be described outlining the ways data may be shared.

This framework describes increasing access to data with ever fewer restrictions:

- **The data set exists** – no detail may be provided other than the existence of the data set. For example, knowing that a register of drivers' licences exists
- **Details about the data set** – such as sharing details of the scope, parameters involved (often referred to as the data dictionary), period over which the data is collected
- **Ability to interrogate aggregated, perturbed, or obfuscated data** – such as the ability to run a defined set of logical operations over, and receive a result from, data which has been de-identified in some way without accessing the data itself. Access may further be refined through the level of aggregation, perturbation, or obfuscation.
- **Ability to access aggregated, perturbed, or obfuscated data** – the ability to run an unlimited set of queries over data which has been de-identified in some way
- **Access to data** – whilst this may still be restricted to certain individuals, for certain approved purposes in secure operating environments, there is no technical limitations to the operations which may be performed

- **Ability to share data** – some systems, such as the SURE[6] system used by the SAX Institute system, limit how data is accessed to prevent further sharing. The ability to on-share data provides the most open access and greatest risk, as has been seen with Edward Snowden and WikiLeaks[7].

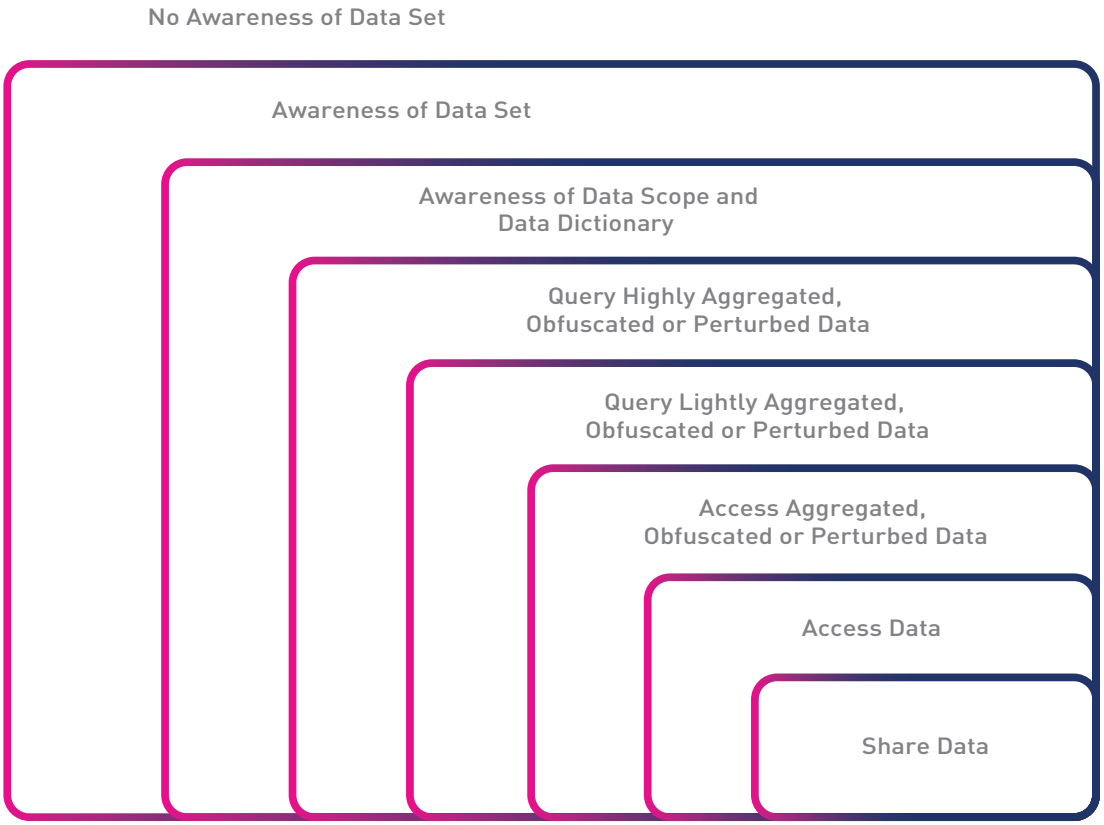
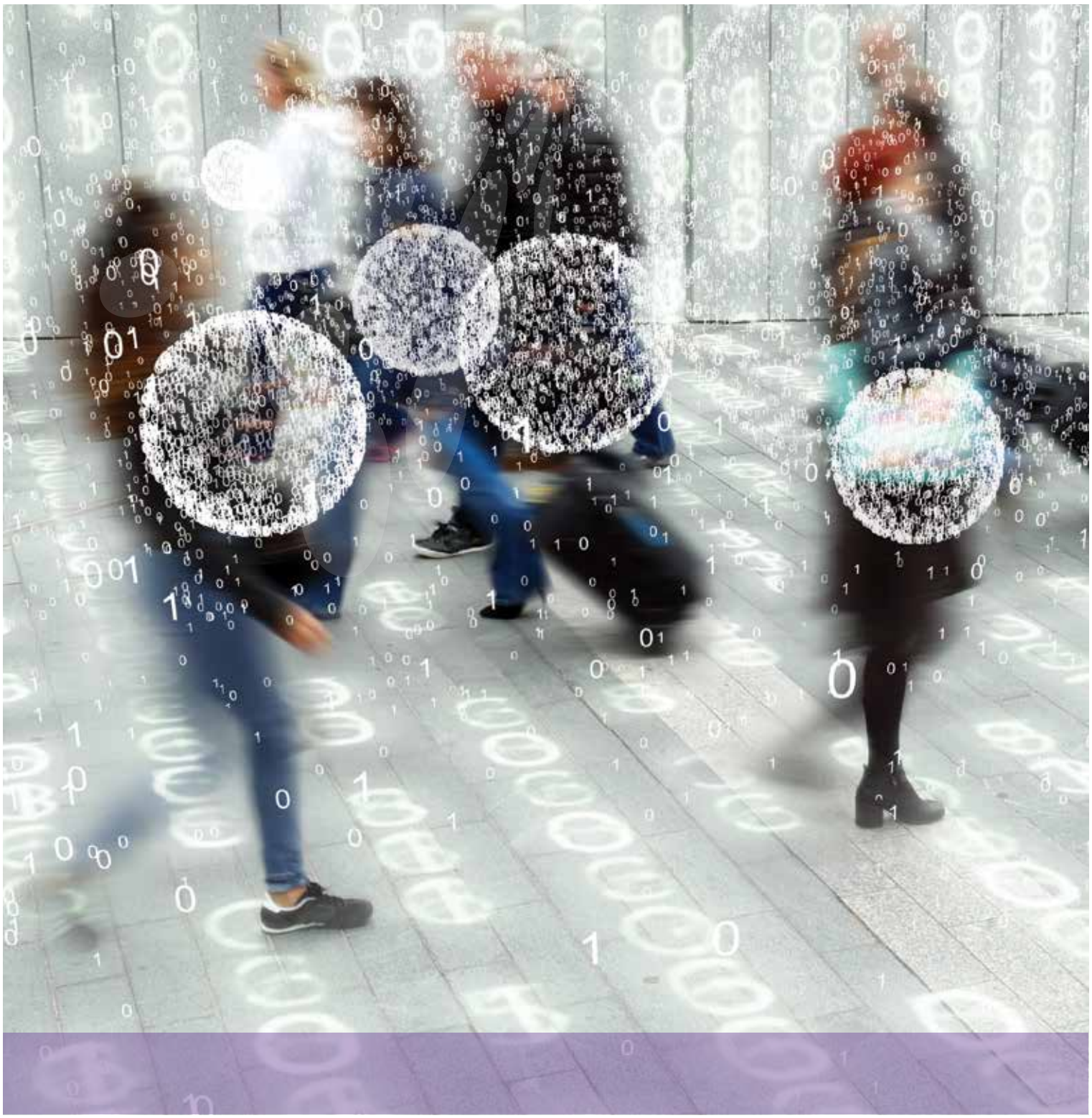


Figure 2. Basic data sharing framework

In this basic framework, there is an explicit assumption that data sharing involves a data source, a data recipient, and a sharing mechanism. It also implies increasingly open access to data to the ultimate point of being able to on-share.

6. For more information see online https://www.saxinstitute.org.au/our-work/sure/
7. See for example Wiki page https://en.wikipedia.org/wiki/Edward_Snowden

05



Valuing Data in a Digital Economy and a Digital Society

Data can arguably be said to have no inherent value. The value of data ultimately depends on how it is used. The near limitless reproducibility and reusability of data, the low cost of storage and transmission, coupled with a high degree of software automation, have changed the number and ways data can be used, and so the potential value of data.

For digital economy companies, data has become one of the primary factors of production as well as a means of customising service delivery. Modern services are increasingly created, delivered, and consumed via digital means.

The delivery and consumption of services in digital format greatly expands the geographic reach of service providers, crossing state and national boundaries, and allowing massive levels of data aggregation. The combined effects of the dramatic reduction in the marginal transaction and delivery costs of digital goods and services – coupled with the reduced costs to consumers of access, discovery, and comparison of goods and services – are driving the world towards a single global market place.

Digital economy companies can also develop extremely high levels of customer intimacy based on 'metadata' generated around search, purchase, shipment, use, user experience and feedback of digital products and services.

5.1 DATA VALUATION FRAMEWORKS

When the outputs of production are digital services rather than physical products, and the major inputs are data and digital services, the traditional model of understanding value becomes stretched. Attempts have been made to create models of the value of data based on benefits to business operation, the cost of replacing data if lost, the impact data has on business decisions, the willingness of others to pay for data held by a business, and new opportunities which could be created if the data is used in different ways.

5.1.1 COMMERCIAL DATA VALUATION FRAMEWORK

The framework shown in Figure 3 has been adapted from the Gartner data valuation framework model[8] and attempts to make explicit possible ways of quantifying the 'value' of data in a commercial context. One of the most fundamental 'value' parameters described in this model is the *Intrinsic Value*. Gartner describes this in terms of accuracy, accessibility and completeness, and it provides a measure of the reliability of data rather than economic value created. Other value parameters attempt to quantify operational uses of data or economic aspects of data.

An important addition to the Gartner model is the *Exclusivity Value of Data* which focuses on the consequences of a loss of exclusivity of a company's data through deliberate or inadvertent release. This may mean loss of commercially sensitive information, or the release of personally sensitive information about staff, vendors, or customers. This in turn may lead to loss of revenue, increased costs, or creation of legal liabilities. A further addition is the *Growth Value of Data* which refers to the potentially limitless opportunities to create new value by combining commercial data with third party data sets.

8. See *Introducing Infonomics: Valuing Information as a Corporate Asset*, Gartner, 2014. Summary available online https://www.gartner.com/doc/1958016/introducing-infonomics-valuing-information-corporate

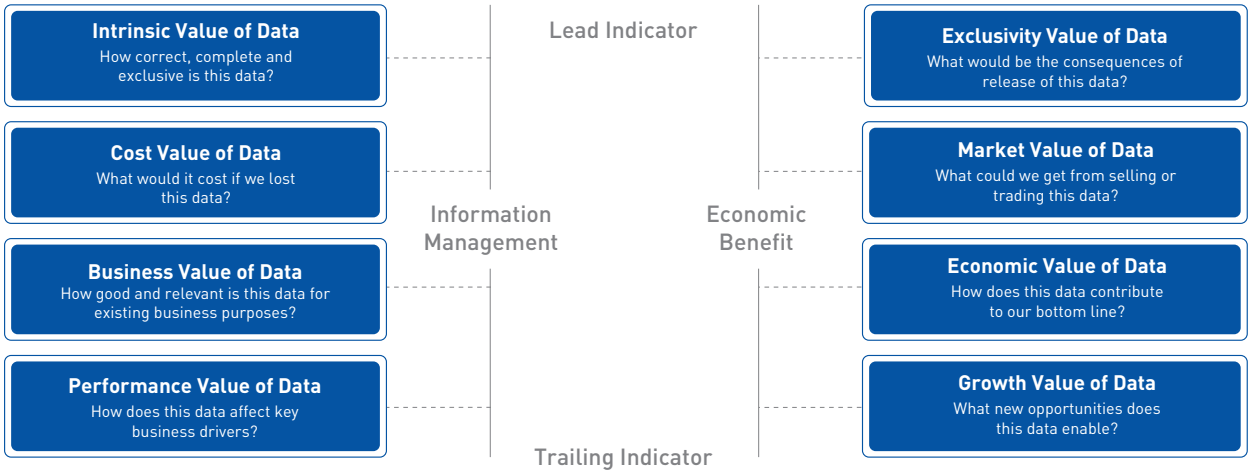


Figure 3. Commercial Value of Data

Data In The Real World

Thomson Reuters is the world's largest historical market data provider offering fine grained market activity (microsecond transactions) in the form of un-manipulated recorded trade and quote messages[9]. This data was originally a by-product of trading activity and was not seen as being intrinsically valuable. Today, data is collected from all exchanges around the globe, and delivered to academic researchers, hedge funds, algorithmic traders, and regulators. A single day's data can range from hundreds of gigabytes to a terabyte.

The high levels of software-driven automation means the exact same data product can be consumed by 100 or 1000 customers with minor adjustments to staff levels, office space or computing resources.

As the use cases grow for the data, the exact same data sets can be used repeatedly without impairing the value of the original. The same data can be used for academic research, training of high frequency trading algorithms, market research or as the raw material for assessing market efficiency. With an appropriate licence agreement, a user of the market data can also on-sell the exact same data for a completely different purpose.

9. See company website for further information http://thomsonreuters.com/en/products-services/financial/quantitative-research-and-trading/tick-history.html (Accessed 6 August 2017)

5.1.2 GOVERNMENT DATA VALUATION FRAMEWORK

For governments, the value of data may be reframed to consider not just operational and policy improvements from the use of data, but the economic stimulus which can be created by deliberate release of data.

Governments hold vast quantities of personal data on citizens, as well as data which is of importance for national security. In modified Gartner framework for government (see Figure 4), the *Exclusivity Value of Data* must consider the impact of the release of highly personal information and issues of national security. Such estimations would be extremely difficult to quantify.

The *Research Value of Data* focusses on research areas which would be enhanced by deliberate release of data under controlled conditions (selected research partners or by anonymising data). In areas as complex as health and human services, access to data held by governments will be critical to understanding and addressing some of the greatest challenges facing Australia. The challenge is of course that this is potentially the highest risk / most sensitive data held by government.

The *Economic Value of Data* focusses on industries which would be stimulated by release of government data with appropriate treatment to prevent personal information from being released.

The *Market Value of Data* focusses on new industries which may be created by release of government data under the same circumstances.

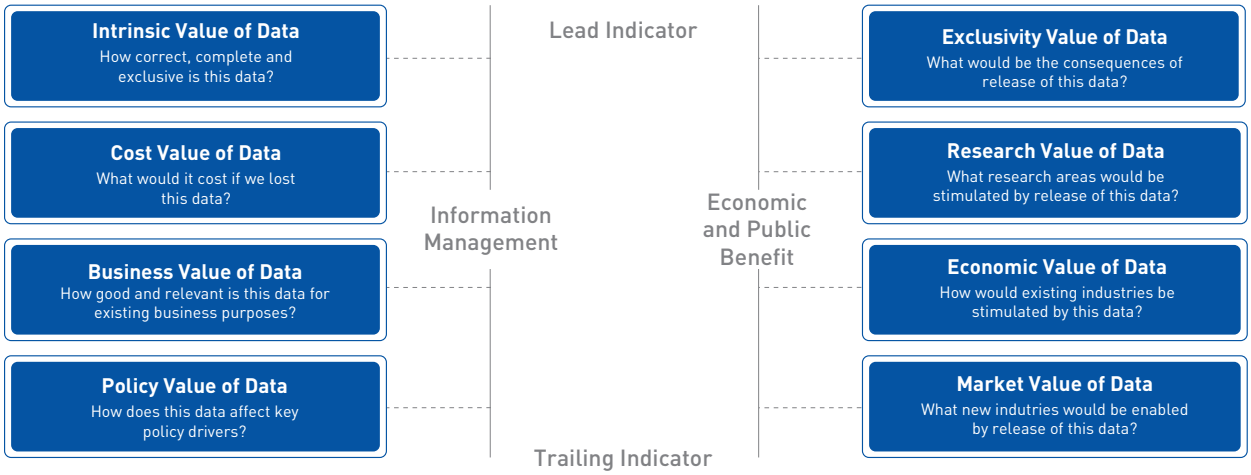


Figure 4. Value of data to the Government and the Economy

With the challenges associated with recognising the value of data, and quantifying the potential risk of release of data, it is not surprising that so many individual data custodians are paralysed by concerns about the consequences of releasing or sharing data. It is also not surprising that, without an accounting framework for data in an accounting sense, that data is undervalued as a factor of production in the Digital Economy.

Data In The Real World

The Health Sector, including provision of aged care services, overtook the Retail Sector in 2011 as the largest employer in Australia and yet it continues to struggle with growing challenges in health service delivery. Despite the estimated spend of $162b in 2014-15[10], the sector faces long-term challenges including the changing case mix driven by Australia's ageing population, and substantial increases in levels of chronic disease.

Three significant developments over the past five decades make this a major public policy and economic challenge: first, the developments within our healthcare system to address all types of diseases with interventions and pharmaceutical support to reduce their impact on quality of life and life expectancy; second, lifestyle changes dominated by the rise in chronic health conditions such as diabetes, cardiac conditions and their resultant negative impacts on health and workforce productivity; and finally, increased life expectancy of an ageing population with more than one chronic condition.

Bridging the gap between innovation and adoption will be critical to addressing this growing challenge. 'Health care' is such a complex combination of systems that modelling and simulation – the flow of patients through the health care system, changes to payment systems, the introduction of new technologies or treatment procedures, and construction of new hospitals – are critical components of future planning, similar in many ways to clinical trials. Datasets and knowledge are the foundations to ensure that we are focused on the most critical and valuable interventions to transform delivery.

A 'citizen centric', integrated care system requires the joining of available data sets to ensure that trial and error is not the basis of change.

The data sets which would drive the greatest change include:

- Health Workforce data
- Medicare and PBS data
- Public and private hospitals data
- Health insurance claims data
- Disability data
- Mental health data
- Residential aged care data
- Community aged care data
- Data on key health and aged care

These data sets are the most valuable in addressing the challenges in the Health Sector as they would allow modelling and simulation trials to test new forms of service delivery, including the impact of telehealth.

10. AIHW, *Health expenditure in Australia 2014-15*, October 2017. Available online http://www.aihw.gov.au/WorkArea/DownloadAsset.aspx?id=60129557188

5.1.3 PERSONAL DATA VALUATION FRAMEWORK

A fundamental consideration for all data sharing is the value of data to the individual. In the commercial framework outlined above, the considerations largely address the use of data in operational (or strategic) considerations, and what economic value could be created or lost from sharing of the data.

The modified Gartner framework for value of individual data is shown in Figure 5.

In the commercial and government frameworks, the operational and strategic considerations are similar. The costs of loss of exclusivity relate to the national or personal security considerations. The unmet opportunities relate to research or industry areas which would be stimulated by release of data.

In both cases, determining the cost or value will require consideration of the impact on individuals. When considering this from the individual's perspective, 'value' to the company or the government may be considered a 'cost' in the form of an encroachment on privacy (impacting the loss of *Exclusivity Value* aspect), or release of information which the individual may otherwise have been able to create value from (impacting the *Market Value* aspect). For example, a better targeted, more personalised, or more customer centric service comes at the cost of sharing personal information on service use, preferences, interests, or personal circumstances.

The impact (or cost) of an individual instance of sharing personal individual data is difficult to estimate except in the most extreme circumstances. The concern about companies or governments sharing personal data for secondary purposes[11] may however lead to individuals deciding to opt-out of service use.

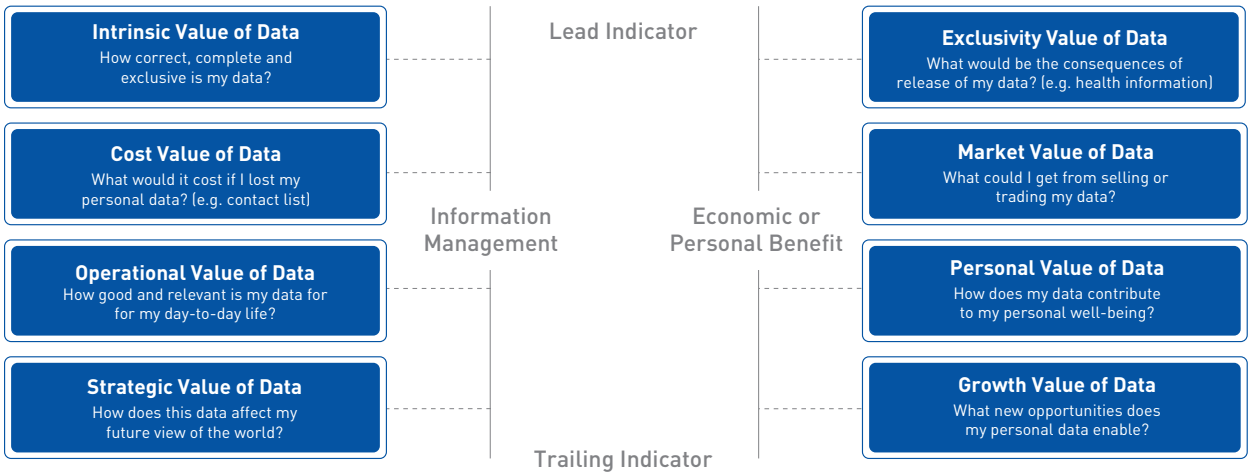


Figure 5. Value of data to the Individual

11. Secondary purposes are anything other than the originally intended use of the data whether aggregated or not.

5.2 VALUE OVER TIME

One of the implicit assumptions of data sharing is that value decreases with the passing of time. The more immediately data is available, the faster the information carried in the data can be used. But the question arises, it is necessarily the case that the 'value' of data decreases over time? The answer is highly dependent on the use case and the information that the data captures.

Data which can be used for longitudinal studies continues to hold value over time as does data used for historical studies.

In financial markets, trading data made available in real time is considered highly valuable and can be costly to acquire both from an infrastructure perspective and from a licencing perspective. This data can be considered a time-series, which records events occurring in a financial market. The interplay of events is of great significance for traders and regulators alike.

In the case of the Australian Stock Exchange, the same data as is sold at a premium for real-time supply, is made freely available after a 20-minute delay. Real-time data is used to drive real-time buy/sell decisions. Near-real time data may be used to confirm trades, assess overall trading position, or validate trading strategies. The historical data retains value for training robo-trading algorithms. Some of the most sought-after historical data is associated with extreme market movements (so called 'Black Swan' events)[12].

Figure 6 depicts a view of 'value' of data over time. After an initial decline in value associated with delay from real-time, the increase in value then comes from the information contained in historical events. The value of these 'High Information Events' may diminish over time but are unlikely to become zero value.

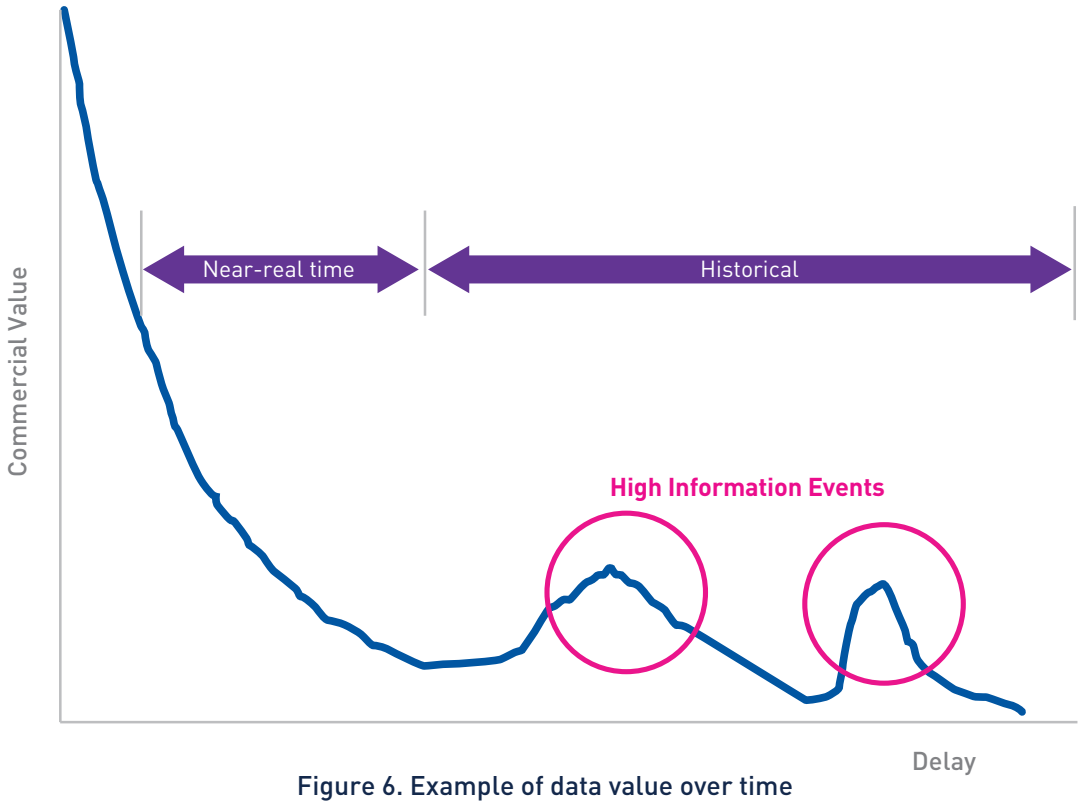


Figure 6. Example of data value over time

12. The concept of 'Black Swan' events was popularised by the writer Nassim Taleb in his book, *The Black Swan: The Impact of the Highly Improbable* (Penguin, 2008). The essence of his work is that the world is severely affected by events that are rare and difficult to predict. The implications for markets and investment are compelling and need to be taken seriously.

The example above presents the changing value of data related to discrete events over time. As the market continues to trade (and possibly even grow in volume), the total data set will grow and capture more high information events. Assuming the real-time and near-real time sections of this growing data set remain valuable, and assuming the historical high information events do not reduce to zero value, the growing data set which contains these events will continue to increase in value over time.

06

Sensitivity – 'A Personal Information Factor'

A fundamental challenge for the creation of smart services is addressing the issue of whether a set of data sets contains personally identifiable information. Determining the answer to this question is a major challenge, as the act of combining data sets creates information.

6.1 WHAT IS PERSONAL INFORMATION?

Personal information (often also called personally identifying information (PII) or personal data) covers a very a broad range of information about individuals. In principle, it covers any information that relates to an identifiable, living individual, where identifiability is determined not only by reference to the information itself, but also having regard to other information that is reasonably available to any entity that holds relevant information. Data protection laws in different jurisdictions (including states and territories within Australia) have adopted different definitions. Courts in those jurisdictions have interpreted these definitions in inconsistent ways. The following brief summary is therefore of necessity, high level only.

In the European Union[13], personal data means:

> *"...any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

In Australia, the definition of 'personal information' differs between the Federal Act and some Australian State and Territory Acts. The current Federal Act uses a different definition to that originally included in the 1988 Act.

The current definition in the Federal Act is:

> *"information or an opinion about an individual, or an individual who is reasonably identifiable, (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not."*[14]

13. Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("General Data Protection Regulation" or "GDPR"), available at www.ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. A more conveniently searchable format of the GDPR is available at https://gdpr-info.eu/. (Accessed 6 August 2017)
14. Privacy Act 1988 (Cth) s 6(1). See also Office of the Australian Information Commissioner, "What is Personal Information?", May 2017, at https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information. (Accessed 6 August 2017).

Taking a state level example, guidance from the Queensland Office of the Information Commissioner makes clear that:

> *"...personal information is defined in the Queensland Information Privacy Act 2009 as 'information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.' It includes information which directly identifies an individual and information that can be compared or cross-referenced with other information to identify an individual. Appropriately de-identified data is no longer linkable to an identifiable individual, which means it is no longer personal information. Once it is no longer personal information, the IP Act does not apply to the data."*

A crucial element in these definitions is that personal information must be *'about an individual .... who is reasonably identifiable'*. Whether an individual is reasonably identifiable requires a context specific inquiry.

6.2 IS PERSONAL INFORMATION PRESENT IN DATA?

Data sets that do not identify particular individuals may be used to create personally identifiable information, if other data sets are accessed which enable identification of the individuals to whom the shared data sets relate.

This other information might be available either:

- **Internally** – for example, by looking up another data set and cross-matching transaction data sorted by transactor key or device identifier
- **Externally** – such as re-identification of individuals through matching of data sets through use of searchable databases such as ASIC records, Land Titles Office property records or through search engines.

Another entity might hold the same 'non-facially' identifying data sets but:

- Without other internal data sets which would enable identifying lookups

  and

- Subject to safeguards and controls which are likely to be effective to prevent access to external identifying information.

Such an entity would not hold personal information about identifiable individuals. However, if that entity elected to release (disclose) that data in circumstances where recipients could reasonably reidentify an individual within that released data set, the entity ***would*** have disclosed personal information about individuals in that facially de-identified data set.

Accordingly, whether data sets relating to individuals that are not expressly identified are personal information about those individuals requires a context specific inquiry as to who holds the relevant information, and the nature of relevant identification reasonably available to that entity.

An entity releasing information in purportedly de-identified form must therefore consider the nature and extent of other information available, and potentially usable by reasonably anticipated recipients of that released data set in order to reidentify any individual that is the subject of that facially non-identifying released data.

It follows that an enquiry must be in two stages:

1. Is personal information about individuals present in data sets as handled by a particular entity having regard to potentially identifying other information, reasonably available to that particular entity
2. Is personal information about individuals present in data sets as released by that entity, having regard to potentially identifying other information, reasonably available to anticipated recipients of that released data set.

For the purposes of this document we will use a hypothetical parameter, the 'Personal Information Factor' (PIF), which is a result of the:

- Personal information content of each of the individual data sets used to create a service (the simplest service may be data sharing)
- Functions which operate on the data sets (such as logical operations or other processing) to produce insights and models
- Individual knowledge of the observer of the insights or models
- Additional information available to the observer that the observer could bring to the insights or models.

Note: The personal information content of each of the individual data sets, and the PIF remain to be defined.

Figure 7 shows the context for evaluating the degree of personal information in a closed system, taking into considered only the first two factors outlined. As an example, consider an information service which determines the number of people who arrive at each train station in NSW, for each hour of the day, for different passenger types (student, pensioner, adult). Using de-identified input data sets, such as service may deliver the insight that on certain days, at one regional station, there is only a single pensioner who alights between 6:00pm and 7:00pm.

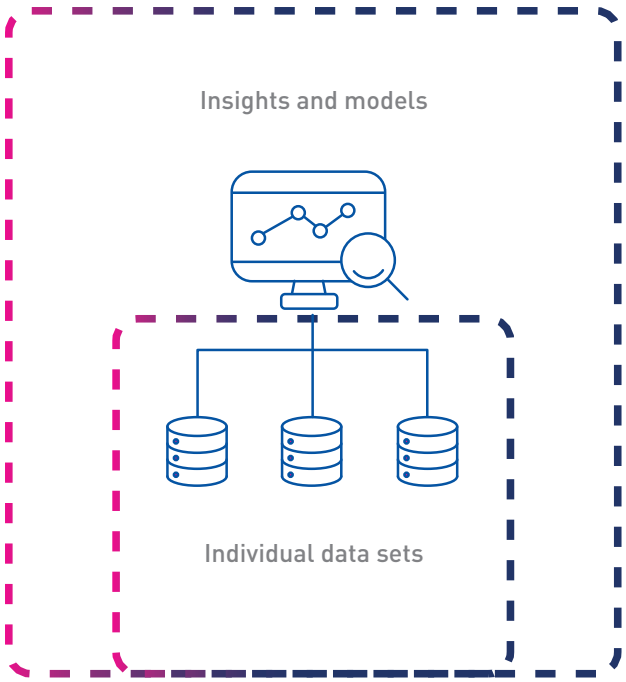


Figure 7. Closed system context for evaluating PIF

Figure 8 shows the context for evaluating the degree of personal information when considering the knowledge of the observer who has their own knowledge of the world. Extending the example above, if the observer has personal knowledge of the regional station identified, and knows several pensioners who live nearby and who travel by train, then the PIF associated with insight produced by this service is increased.

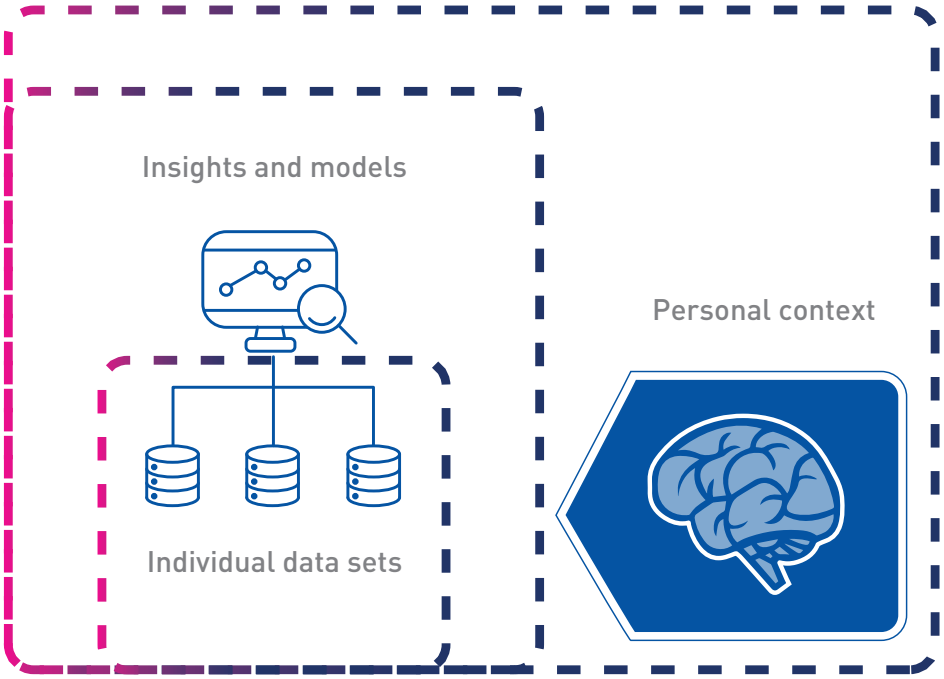


Figure 8. Human context for evaluating PIF

Figure 9 shows the framework for considering PIF in an insight when additional information can be brought into the context of information/data which has been shared. Extending the example above, if the observer has personal knowledge of the regional station identified, and knows several pensioners who live nearby and who travel by train, and waits at the station on the days the individual is known to travel, then the PIF associated with insight produced by this service is increased to the point where the individual travelling pensioner can be identified. Specifically, the PIF can be brought to 1 (100% personally identifiable).

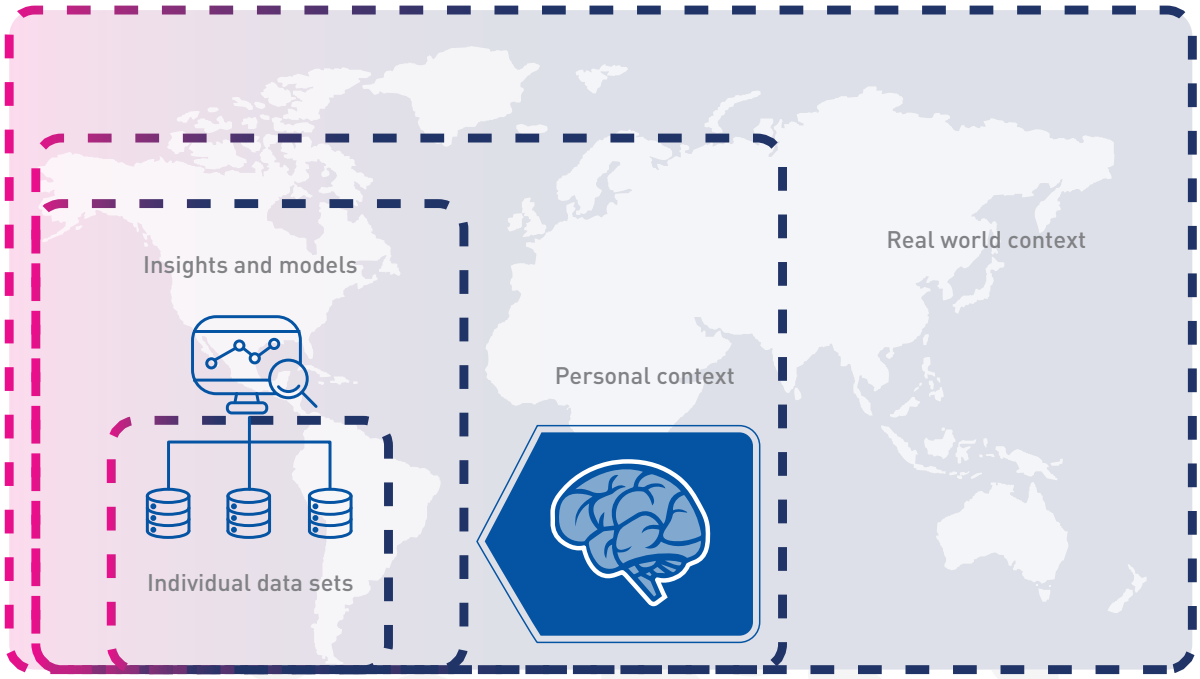
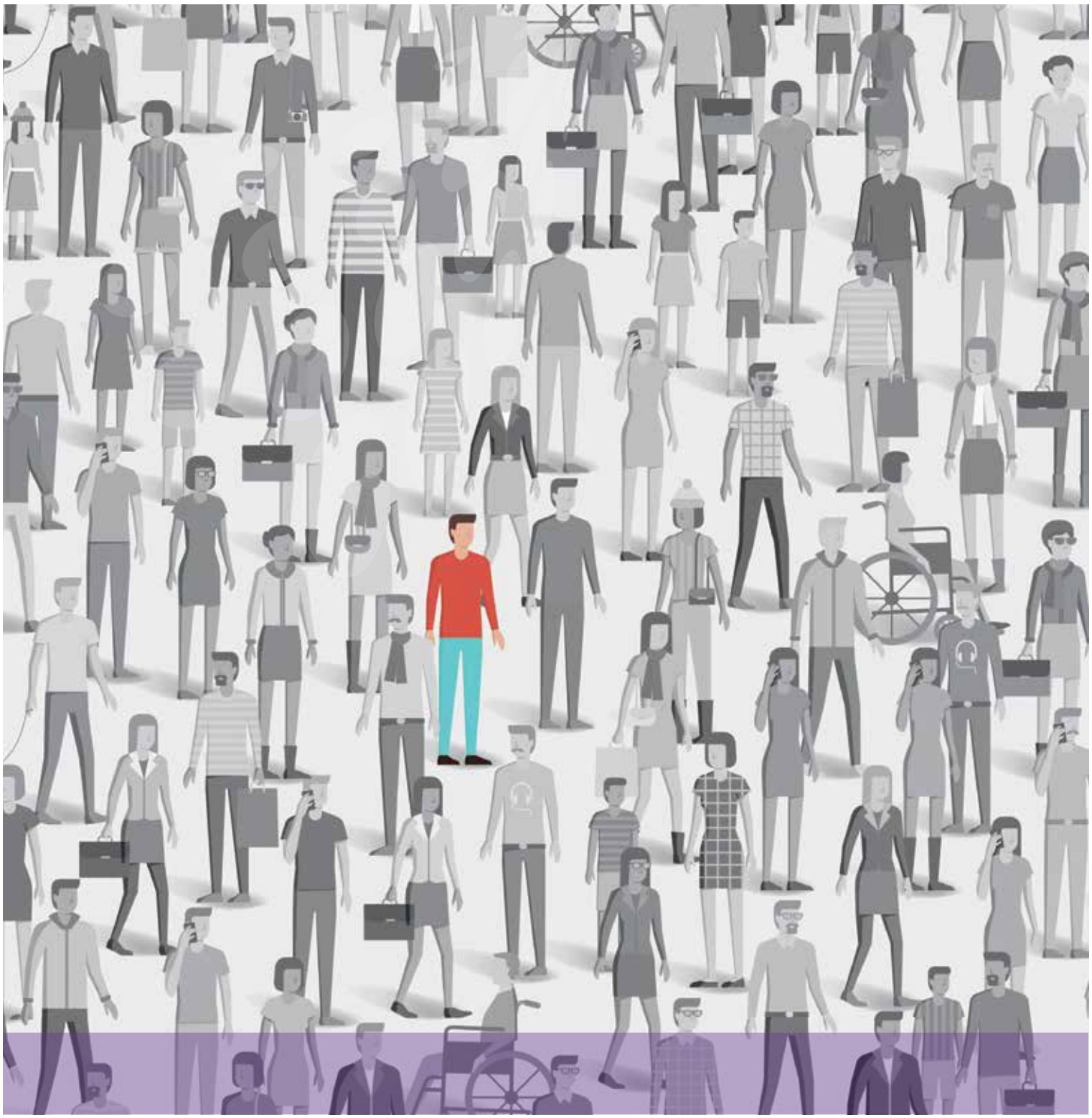


Figure 9. Real world context for evaluating PIF

While the example of the travelling pensioner may seem trivial, it highlights the technical, social, and contextual challenges associated with data sharing. What has high information content for one observer may have low information content for another. What in a limited context is the identification of any single individual ('any' anyone), may become identifiable with an actual individual (an actual 'someone').

07



A Framework for 'Reasonable'

Throughout this document, we have used personal information as information or an opinion about an individual who is reasonably identifiable, following the current definition in the Federal Privacy Act.

This definition ignores the distinction between data and information. In this document, we use the working definition that 'Personal Data' is that which contains personal information about an individual (high Personal Information Factor), or which is or readily could be combined (by the current holder of that information or, in the case or release, by any reasonably anticipated recipient of that released data set) to create personal information about an individual (has a non-zero Personal Information Factor).

Examples of Personal Information cited on the website of the Office of the Information Commissioner[15] include:

> *An individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person.*

Of these examples, it is easy to see how some could be used to identify an individual:

- After formal identification, a copy of an individual's signature may be kept on record by a 'trust' centre such as a bank and used to reidentify that individual in future
- After identification, formal data handling and governance processes are used to manage collection and use of medical records, ensuring the same individual is always associated with the same data.

Whilst they may contain some personal information, the other examples put forward are less clearly associated with being able to identify an individual:

- Each of us has only one date of birth, but many people share the same date of birth. Whilst it may be used as one factor for identification, date of birth with no other information cannot be used to uniquely identify an individual (low Personal Information Factor).
- While a person typically has one legal name, many people share the same name. Like date of birth, with no other information, cannot be used to uniquely identify an individual (moderate to low Personal Information Factor). An individual may have a set of commonly used nicknames or aliases, and many online identities in different contexts (low to very low Personal Information Factor).
- Telephone numbers – once associated with a fixed residence and published in White or Yellow Pages directories – are now automatically allocated each time a prepaid SIM card is purchased and may have a useful life of only one call or data connection (low to zero Personal Information Factor).

15. See Office of the Australian Information Commissioner website https://www.oaic.gov.au/privacy-law/privacy-act/ (Accessed 6 August 2017).
See also Office of the Australian Information Commissioner, "What is Personal Information?", May 2017, at https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information. (Accessed 6 August 2017)

The level of personal information associated with a telephone number has changed with the changing use of telecommunications from person-to-person communications, to being an entry point to the Internet of Things. A telephone number may have a high Personal Information Factor if there is strong or long-standing association with that individual. It will have a low Personal Information Factor if the number is used only once, shared amongst many people, or used by an anonymous device in the possession of the individual.

Names have an even more interesting relationship to Personal Information Factor. In some close-knit communities, combinations of given and family names can be quite common as a result of tradition. In Griffith NSW, for example, the surnames Sergi and Catanzariti are very common and there are a relatively small number of given names. Tradition states that the oldest son should be named after the paternal grandfather, the eldest daughter named after the paternal grandmother, and then the second oldest of each child being named after the maternal grandparents.

This leads to many people with identical legal names and the proliferation of nicknames to try to distinguish individuals with the same legal name.

In the seventies, the Woodward Royal Commission[16] referred to key players of the Griffith community by their nicknames rather than their legal names. In reporting on the Royal Commission, both the ABC and the Daily Mirror were successfully sued for defamation where they displayed the photograph of the 'wrong' Patrick Sergi because they assumed that the name was relatively unique, and did not check the nickname. Conversely, the nicknames used within the local community such as '7 Tonne', 'Biscuit', 'Crumbs' or even 'Jingles' shed little light on the identity of the individual for those outside of the community.

Taking another perspective, if an individual used their legal name to register for online services such as provided by Skype, LinkedIn, Twitter, Tinder, or Ashley Maddison, this can be personally identifiable. If however, an individual created a different online persona for each of these services, it may not be possible to identify the individual. Knowledge of the set of personas may however be used to identify the individual.

Taking the question of what is personal information further, the questions associated with identification of an individual from data they create, or the data sets which contain information about them, are broadly categorised as:

- **A Cohort of One** – is identifying an anonymous individual (person, company, entity) the same as identifying the individual?
- **Radius of Convergence** – if ever more data sets are brought together, is it certain that personal information will be reached or that an individual will be identified?
- **Uniqueness** – how small a cohort is required before an individual can be uniquely identified?

When 'reasonably' is used as the test, the framing question becomes: what is the limit on the ability to decide if personal information is present when increasingly more data sets are brought together?

And finally, if we can find answers to these questions above, could we develop automated trust frameworks with measurable units of 'trust'?

16. See NSW State Archive https://www.records.nsw.gov.au/agency/2125?title=Sergi

7.1 A COHORT OF ONE – IDENTIFYING 'ANY ANYONE'

Privacy legislation is framed in terms of identification of an individual. In the case of NSW privacy legislation, it need not even be a living individual – covering people up to 30 years after death.

Data anonymisation is often used as a means to prevent dealing with personal data. A fundamental challenge however is faced when exploring cohorts of people in data sets which begin to narrow to individuals. Online advertising may be shaped based on individual preferences and browsing behaviours, in-game promotions may be targeted based on gaming behaviours.

The value of these focused services is clear. The challenge however is if narrowing service delivery to the anonymous individual is the same as dealing with a named person. Is the identification of a 'cohort of one' the same as identification of an individual person?

▶ **Is the identification of a cohort of '1' the same as identification of an individual person?**

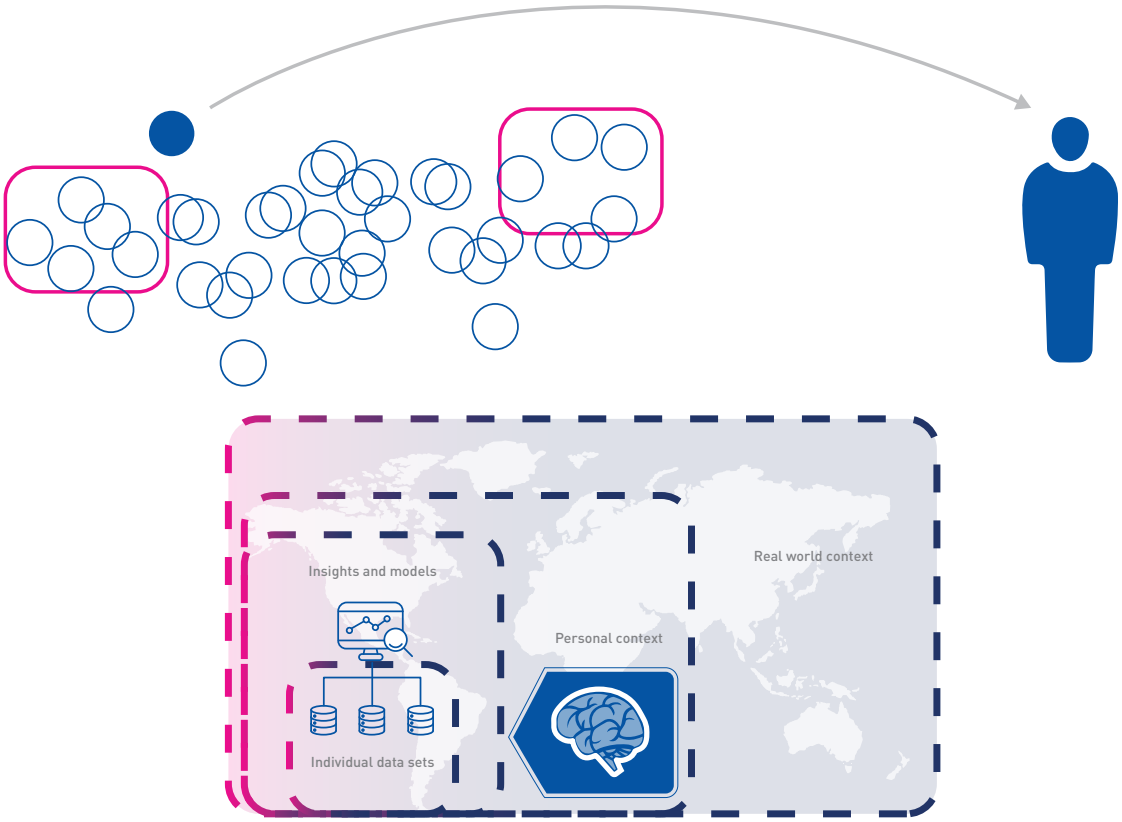


Figure 10. Identification of an anonymous individual, and the potential to link to the person

Framing questions:

- What are the circumstances required to unambiguously connect a cohort of one de-identified individual to an individual person?
- What circumstances would prevent the mapping to an individual person?

7.2 THE ABILITY TO DECIDE

People are notoriously poor at making decisions based on multiple inputs.

One of the challenges with a test for personal information described in terms of 'reasonably' is the issue of being able to make decisions about whether data sets contain sufficient information to be able to determine if an individual can be identified.

If data sets contain, for example, date of birth (low Personal Information Factor), then it is possible to think of scenarios where an individual can be identified by adding additional data sets with non-zero Personal Information Factors. If date of birth is linked to postcode (low), gender (low), school attendance (low), dietary restrictions (low to moderate), work location (low to moderate), it is easy to see how this narrowing set of candidates could lead to an identified individual (Personal Information Factor builds to 1).

Framing questions:

- What are the measures a person can use to decide if a person is "reasonably" identifiable?
- What is the limit on the number of data sets a person can mentally process to determine 'reasonably'?

▶ With the linking of ever more data sets, how can judgement be applied?

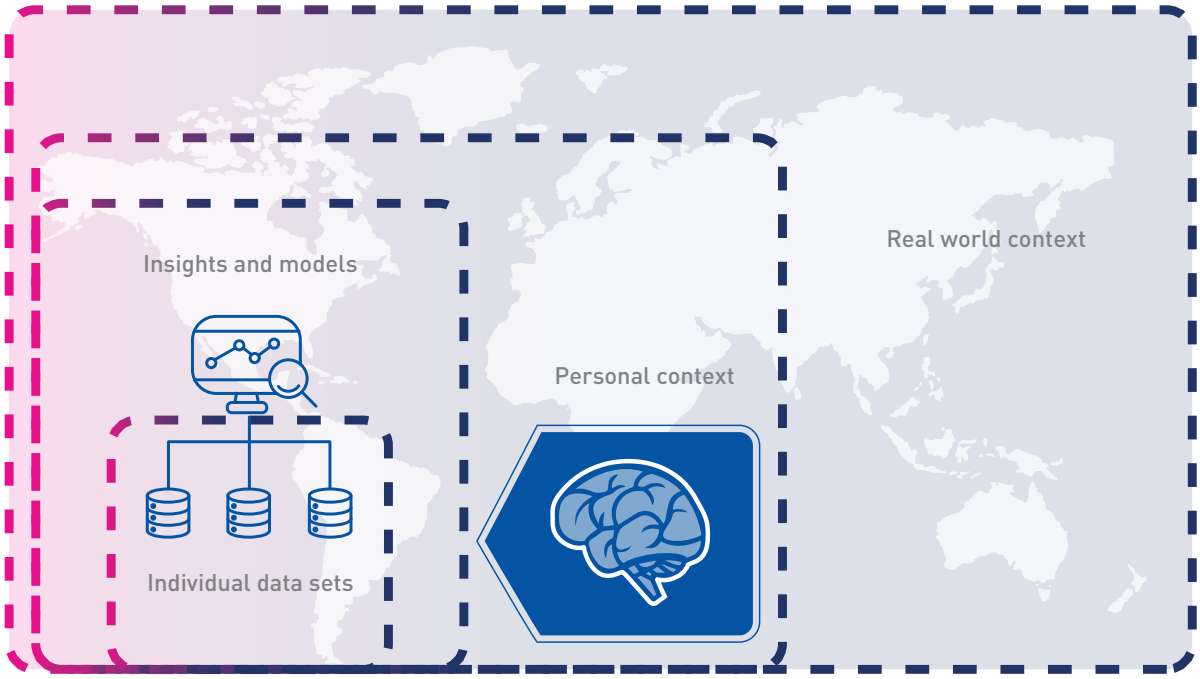


Figure 11. The ability to decide

7.3 RADIUS OF CONVERGENCE

A related argument to that presented in Section 7.2 is the assumption that combining of ever more data sets must lead to the identification of an individual (Personal Information Factor of 1). As with the example provided in Section 7.2, it is possible to imagine scenarios where this is the case: linking home postcode, work postcode, online login name, date of birth, and so on. However, if you combined home postcode plus data with very low (or zero) Personal Information Factor such as weather information for that postcode, you could link data sets spanning the last hundred years without coming any closer to identification of an individual.

▶ **Does the linking of ever more datasets necessarily lead to indentification of an individual person?**

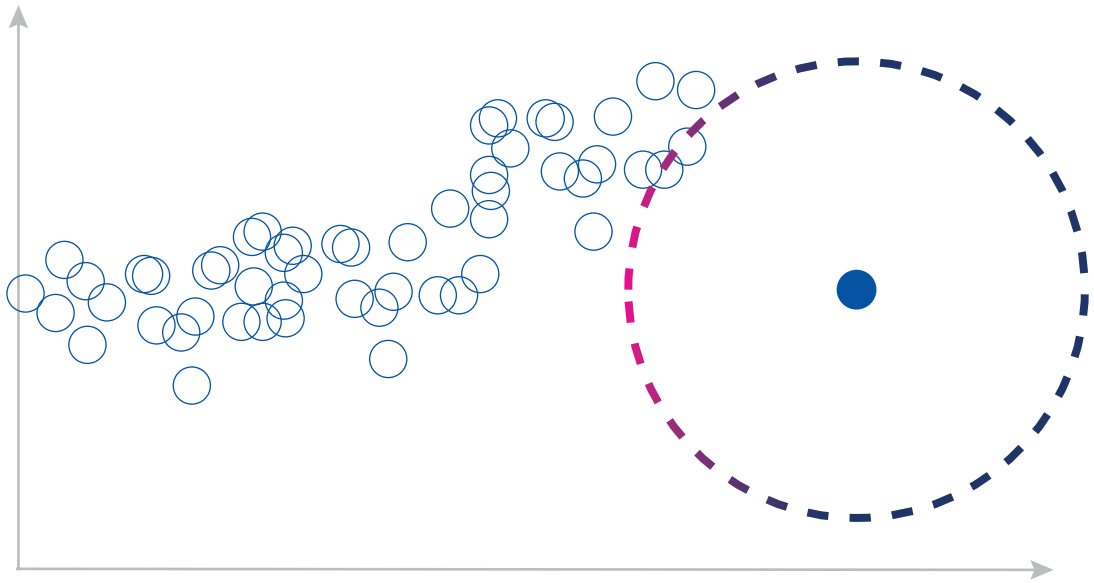


Figure 12. Radius of Convergence

Framing questions:

- Under what circumstances will the linking of ever more data sets lead to identification of an individual?
- What conditions must be met to ensure linking ever more data sets will not lead to identification of an individual?

7.4 HOW UNIQUE IS TOO UNIQUE?

The risk of identifying an individual is often addressed through aggregation of data. For example, data sets which contain age, gender and income may be aggregated to suburb or SA1 level and then released. This risk however is the classical linkage problem where additional, external, data sets are used to dissect an aggregated data set sufficiently to identify an individual (cohort of one). Combining age/has-a-beard/income with religion, marital status, employment type, car ownership, credit card debt, smoking preference, favourite beverage and so on, may lead to a cohort of one.

To use aggregation as a personal information protecting technique, the challenge becomes identifying the feature set which describes the smallest cohort within the aggregated set. Individuals within the smallest (most unique) cohort of the feature set are potentially the most vulnerable to linkage attack. The level of uniqueness of a cohort in a data set can be described in terms of the percentage of the total data set that the individuals in the cohort match.

Taking a real example examined recently, if individuals in a cohort match the entire set, they are not unique (men in a small working group of all men). If an individual uniquely matches one characteristic in a data set (men with beards in a small working group of all men), they can be identified uniquely.

Perturbation is another technique which is often used to limit how small a cohort can be become. If there is uncertainty as to the exact match of features in a data set, it may not be possible to reduce the cohort to one. If, in the example of the bearded male working group, perturbation of the property 'has-a-beard' may be sufficient to limit the unique identifying feature.

▶ How unique is too unique?

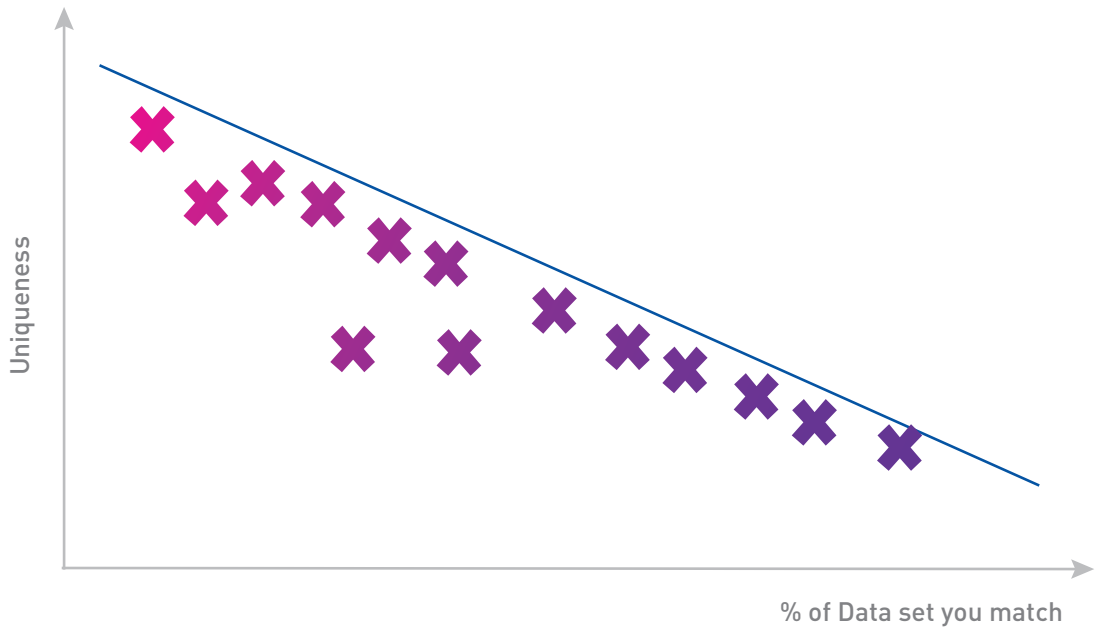


Figure 13. Uniqueness in a set of data

Framing questions:

- How unique is 'too unique' to limit the effectiveness of linkage attack?
- What conditions must be met to ensure linking ever more data sets will not lead to identification of a cohort of one?

08


#include "Units.h"
#include "Savable.h"
#include "WOBox.h"
#include "PhysicsMath.h"
class PhysicsPump: public Savable
private:
float m_qMax, m_pMax;
float m_speed;
float m_stray;
float m_on_;
float m_blocked;
public:
float m_pIn;
float m_zOut;
bool m_cavity;
PhysicsPump();
Properties
float speed();
bool working();
void process(float dt);
void set_p_in(float p_in);
float q();
float dP_filter();
float p_in();
float t_gidropyata();
float p_out();
float dx_val();
float vibr_val();
float t_pump_podsh_pole();
float t_pump_podsh_work();
float t_dvig_podsh_pole();
float t_dvig_podsh_work();
float current();

Frameworks for Describing Services Types

Whilst not universally true, many data custodians are hesitant to share data. This is often due to concerns related to: appropriate use and interpretation of data; concerns about unintended consequences of sharing data; concerns about accidental release of sensitive data; and concerns about adherence to legislation. Frameworks for trusted data sharing would help address these challenges.

Many organisations have limited experience with data sharing and are developing processes on a case-by-case basis. Some organisations have established data sharing processes but they differ from one group to another. Aggregation is often used as a means of reducing the Personal Information Factor in a data set which is to be shared. Aggregation may be based on area (count per suburb or per SA1), over time (count per hour, day, or week), by age (under 18, 18 to 45, over 45). There is however no way to unambiguously determine if there is personal information in aggregated data. Consequently, different levels of aggregation are used by different organisations depending on a perceived value of risk associated with the data to be shared.

A standard protocol for defining requests and establishing data governance would improve the confidence and efficiency associated with data sharing projects.

To help address the challenge, a framework of service types based on use of different data types will be presented. The framework has been developed based on two main contributing factors (represented by different axes): 'Personal Information Factor' and 'Access'.

8.1 EXPLORING BY PERSONAL INFORMATION FACTOR (PIF)

Data with no personal information (public transport timetables) is assumed to have a Personal Information Factor of zero. 'Highly aggregated' data is assumed to have a Personal Information Factor of greater than zero, 'lightly aggregated' is assumed higher than 'highly aggregated' up until the point where personal information is present in non-aggregated data.

Dealing with the Personal Information Factor axis first, the concept of 'services' has been broken into those dependent on four data set types:

- Non-personal data sets
- Above and sets of highly aggregated personal data
- Above and sets of lightly aggregated personal data, and
- Above and sets of personally identifiable data.

Personal data sets that contain health information are not within scope of this exercise as such data is subject to well–defined processes and limitations. Data collected with user consent is also excluded.

Figure 14 illustrates the range of services types considered (dotted boxes) based on the data sets used to create them. The most restrictive data set used to create a service sets the framework for that service. As an example, a service which relies on personally identifiable data as well open data sets will use a framework for services reliant on personally identifiable data. The dotted box in Figure 14 illustrates the region of uncertainty as to the presence of personal data.

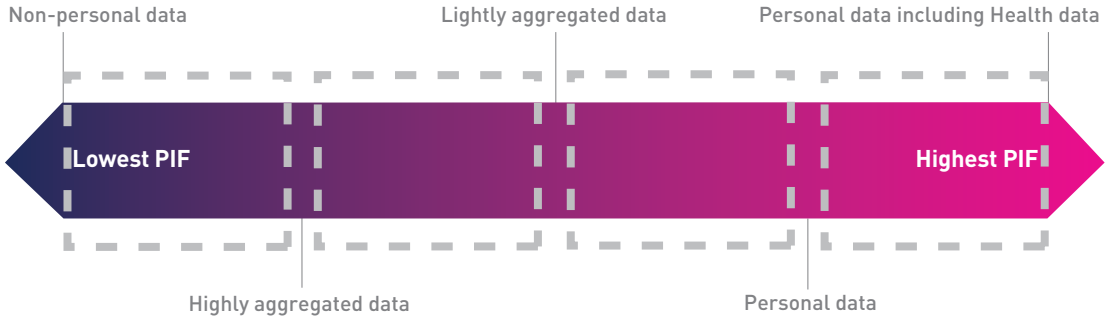


Figure 14. Spectrum of possible service types based on different data set types

This framework attempts to establish the characteristics of service types based on different data set types.

The framing questions which must be addressed per service type are:

- Is personally identifiable information present in the data sets used to create or deliver a service?
- What is the highest Personal Information Factor in data sets required to create a service?
- Under which privacy legislation (State or Commonwealth)[17] can these data sets be collected?
- Under which privacy legislation (State or Commonwealth) can these data sets be shared?
- What are the rights, roles, responsibilities, and limitations for service delivery organisations using this data?
- What changes in context or additional data sets would move a service to a higher Personal Information Factor?
- What are the rights, roles, and responsibilities for the service delivery organisations when a service changes character to depend on a higher Personal Information Factor?

17. In some cases both the State and Federal Act apply: For example, in New South Wales the collection and handling of health (personal) information by private sector health services is regulated under both the NSW Act and the Federal Act.

8.1.1 SERVICES BASED ON NON-PERSONAL DATA

Services based on non-personal data are assumed to have a Personal Information Factor of zero. Bus timetables and historical weather records would easily be characterised as having a very low (zero) Personal Information Factor. Figure 15 highlights the region on the data spectrum used to create services of this type. The threshold of 'highly aggregated data' is arbitrary.

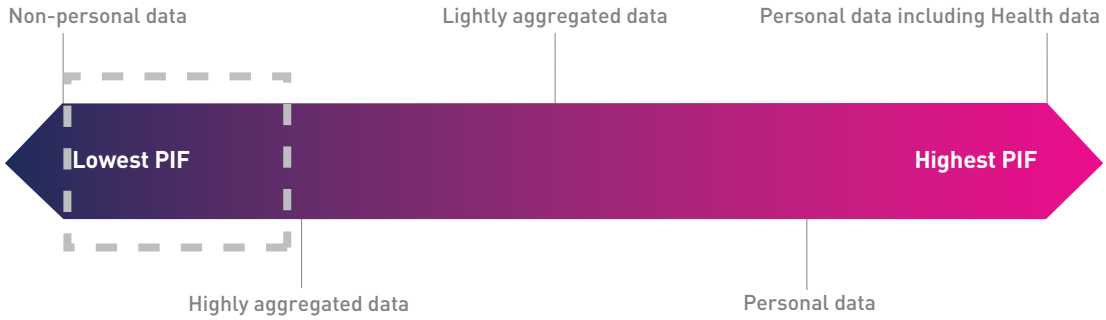


Figure 15. Services based on non-personal data

Framing questions:

- What, if any, are the limitations on services created using non-personal data?
- What is an effective test to ensure personally identifiable information is not present in data which is considered to be 'non-personal'?
- When could a data set without personal information become an important component in a service with a high Personal Information Factor?
- What is an appropriate response when data without personal information becomes an important component in a service with a high Personal Information Factor?

8.1.2 SERVICES BASED ON HIGHLY AGGREGATED DATA

The Australian Bureau of Statistics (ABS) collects data at household level every five years though a national census. The ABS releases data at SA1[18] (statistical area 1) level including Socio-Economic Indexes for Areas[19] (SEIFA) which ranks areas in Australia according to relative socio-economic advantage and disadvantage. This information is used by researchers and industry alike. Aggregating to SA1 level is widely believed to protect the information of individuals because the number of individuals in an SA1 level is relatively high. In total, there are 54,805 SA1s covering the whole of Australia without gaps or overlaps. Figure 16 shows the process the ABS uses to construct SA1 areas.

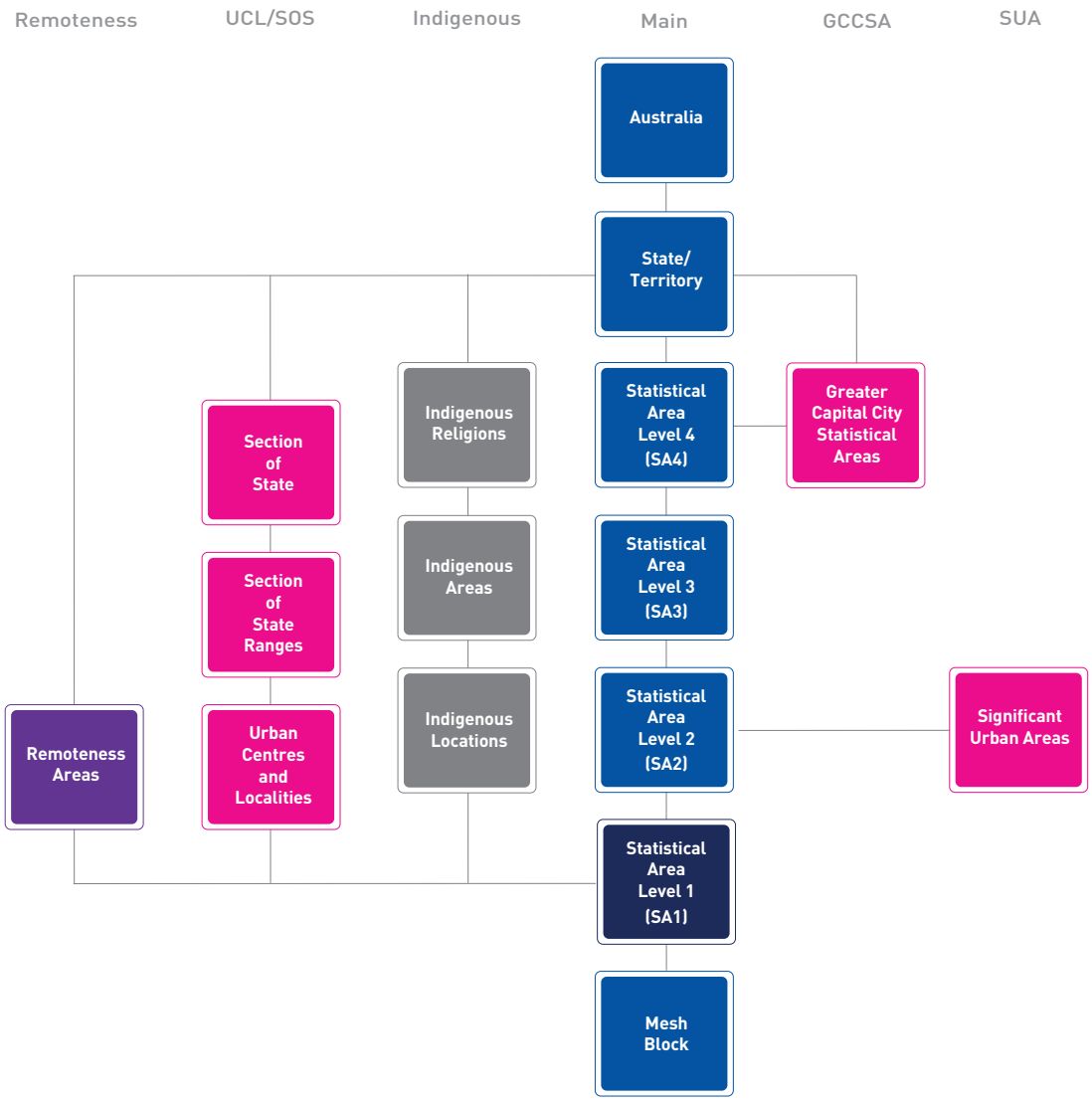


Figure 16. Definition of Statistical Areas according to the ABS (*Source: ABS*)

18. A description of SA1 areas is available online http://www.abs.gov.au/websitedbs/D3310114.nsf/4a256353001af3ed4b2562bb00121564/6b6e07234c98365aca25792d0010d730/$FILE/Statistical%20Area%20Level%201%20-%20Fact%20Sheet%20.pdf

19. A description on SEIFA can be found online http://www.abs.gov.au/websitedbs/censushome.nsf/home/seifa

Figure 17 shows the region on the Personal Information Factor axis for services based on data sets of this type.

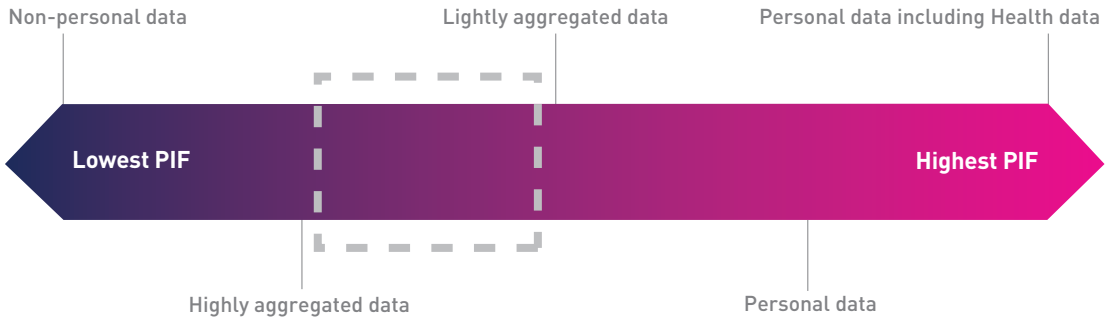


Figure 17. Services based on highly aggregated data

Framing questions:

- What, if any, reduction in Personal Information Factor is provided by aggregating data at different levels?
- What is an effective test to ensure personally identifiable information is not present in data which is considered to be 'highly aggregated'?
- When could highly aggregated data become an important component in a service with a high Personal Information Factor?
- What is an appropriate response if highly aggregated data becomes an important component in a service with a high Personal Information Factor?

8.1.3 SERVICE BASED ON LIGHTLY AGGREGATED DATA

Many organisations default to high levels of aggregation to ensure the Personal Information Factor in the data shared is negligibly low. The potential use cases for data however increase as the granularity of data increases. The greater specificity supports improved understanding of actual situations and of possible interventions when using data at ever greater resolution.

More can be understood and more use cases can be considered if data were available on a monthly, weekly, or hourly basis level than an annual snapshot. The question is always: what level of aggregation provides sufficient protection for individuals whilst still providing the opportunity to inform and create value?

This is the essence of the challenges faced by this Taskforce. Figure 18 highlights the region on the data spectrum used to create services based on lightly aggregated data. The threshold of 'lightly aggregated data' is arbitrary.

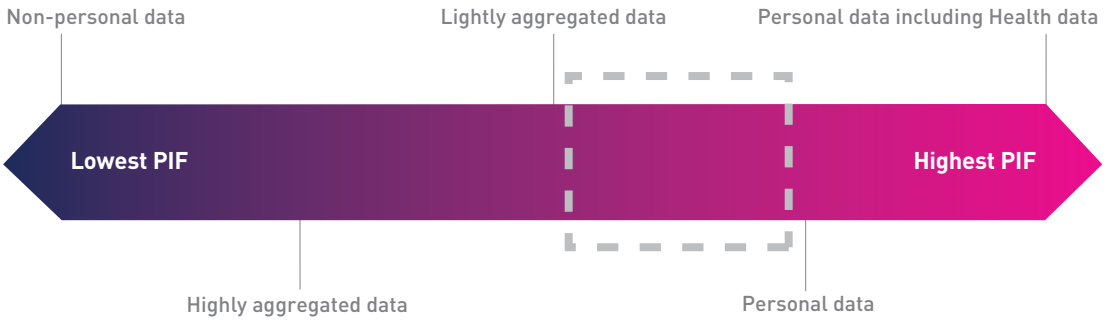


Figure 18. Services based on lightly aggregated data

Framing questions:

- What is the level of aggregation of data required before the Personal Information Factor ceases to be a concern?
- What is a threshold test to ensure personally identifiable information is not present in data which is considered to be 'lightly aggregated'?

8.1.4 SERVICE BASED ON PERSONALLY IDENTIFIABLE DATA

Despite the broad and ambiguous description of personal information, strict provisions apply when data containing personal information is used. Figure 19 highlights the region on the data spectrum used to create services of this type.

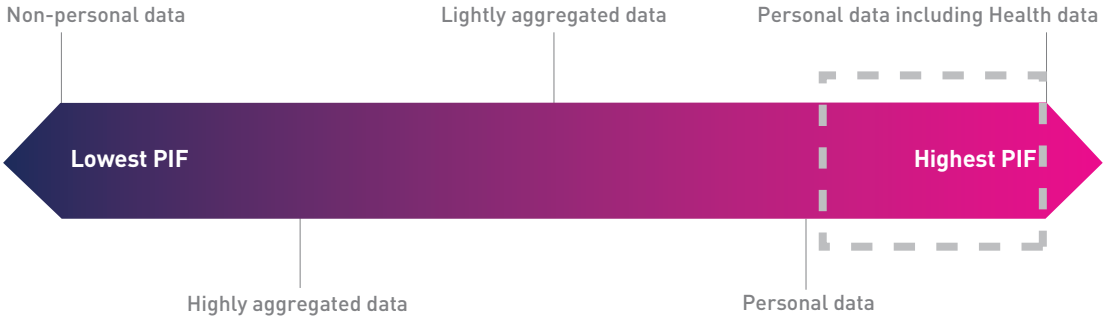


Figure 19. Services based on data containing personal information

Framing questions:

- When is personal information present in data sets?
- Given the ability to search, compare and identify in an online world, what do terms such as 'reasonably' mean?

8.2 ANONYMISATION OF DATA

Anonymisation of data is often considered a means of addressing the concerns associated with the unintended consequences of release of personal data. The Federal government recently released PBS and MBS data providing the research community with the opportunity to explore the longitudinal history of approximately 10% of all Australians. The potential is for researchers to explore some of the most significant challenges of the Australian health care system. The anonymised '10% sample' was quickly removed from the data.gov.au website when a third-party team demonstrated they could successfully reidentify individuals in the sample (an "any anyone" rather than a specific individual).[20]

The Federal government release of 10% PBS and MBS data was an attempt to provide a valuable data set whilst preserving anonymity of the individuals associated with the original data. The most common approaches to data anonymisation are:

- K-anonymity (Medium to weak protection)
- L-diversity (Medium)
- Differential privacy (Strong)

8.2.1 K-ANONYMITY

A data set is said to have the k-anonymity property if the information for each person contained in the release cannot be distinguished from at least k-1 individuals whose information also appear in the data set. There are two commonly employed approaches for achieving k-anonymity (for a given value of 'k'):

- **Generalisation** – where values of selected attributes are replaced by a broader category. For example, age may be replaced by a band from 0-5 years, 5-10 years and so on.
- **Suppression** – where certain values of the attributes are replaced by a null value before release. This is often used for values such as a person's religion.

Because k-anonymisation does not include any randomisation, someone attempting to reidentify an individual can still make inferences by linking other data sets to the k-anonymised set. It has also been shown that using k-anonymity can skew the statistical characteristics of a data set if it disproportionately suppresses and generalises data points with unrepresentative value.

8.2.2 L-DIVERSITY

L-diversity is an extension of the k-anonymity model that uses group–based anonymisation to reduce the granularity of a data representation. The model uses techniques including generalisation and suppression such that any given record maps onto at least k other records in the data. The l-diversity model handles some of the weaknesses in the k-anonymity model where protected identities to the level of k-individuals is not equivalent to protecting the corresponding sensitive values that were generalised or suppressed.

20. The Federal Attorney-General subsequently announced proposed amendments to the Privacy Act and in 12 October 2016 the Privacy Amendment (Re-identification Offence) Bill 2016 (Cth) was introduced into the Senate. As at August 2017, the Bill remained pending.

8.2.3 DIFFERENTIAL PRIVACY

Differential privacy is a mathematical approach which provides a guarantee (up to a pre-determined limit) that the data of an individual will not change the statistical characteristics of a data set whether or not their data is contained in a data set. It maintains the statistical characteristics of a data set by injecting random noise into a data set (which may include reducing an individual's data to zero) and so supports the ability to learn useful information about a population while learning nothing about an individual[21].

Framing questions:

- What are the limitations on services created using anonymised data?
- What is an effective test to ensure personally identifiable information is not present in anonymised data?
- When does anonymised data become an important component in a service with a high Personal Information Factor?
- What is an appropriate response when an anonymised data set becomes an important component in a service with a high Personal Information Factor?

8.3 EXPLORING SERVICES TYPES THROUGH 'ACCESS CONTROL'

As discussed in Section 5.1, the 'value' of data can be framed as a many factored issue associated with business impact, cost, liability, and opportunity. The proxy for value we will use in further discussion is ease of access, or in fact the opposite, 'control'. If there are no barriers to access, then anyone who wants access to data can gain it and so the 'value' of data is assumed to be close(r) to zero. If access to data is heavily controlled, then very few people will have access and so the value is assumed to be higher. This argument is clearly imperfect and is similar to the challenge of placing 'value' on fundamental commodities such as clean water[22].

This 'Access Control' axis is divided into four categories as shown in Figure 20. The authorising frameworks are treated separately. Services based on data 'which cannot be shared without anonymisation' are not considered in this document.

Figure 20. Control or Access types to data

21. See for example C. Dwork, A. Roth, *The Algorithmic Foundations of Differential Privacy*. Available online http://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf (Accessed 6 August 2017).
22. Clean water is widely available through public utilities at low cost in most developed counties and so is often considered to have low economic value. Its absence however creates great cost in financial and health terms. See for example, Global Water Partnership http://www.gwp.org/en/ToolBox/ABOUT/IWRM-Plans/IWRM-Principles/Social-and-economic-value-of-water/ (Accessed 6 August 2017).

8.3.1 SERVICES BASED ON FREELY AVAILABLE DATA

Services based on open data, which is freely available to anyone, are characterised by very few restrictions on those who create, deliver, or consume the service. Data for such services can be accessed without a fee, used many times over in many different ways creating potentially valuable services for which people may be willing to pay.

Examples include journey planners based on public train or bus timetables, or applications which use open government data including weather data, or the recently released Fuel Check application allowing people to track petrol prices in NSW[23]. In these cases, if an application needs to access data 1, 10 or 1000 times to deliver a result, the cost of access remains the same (from the perspective of the data provider).

8.3.2 SERVICES BASED ON DATA AVAILABLE FOR A 'NOMINAL FEE'

Once a fee for cost of delivery is introduced, a limit is placed on how frequently data may be accessed or how many times it can be used for a particular application. If there is a cost per delivery, then much greater value must be created if data is accessed once, ten times or a thousand times to deliver a single result.

Examples of services available for a 'nominal fee' include per location GPS data (the cost is associated with a GPS receiver at each location), and data which is accessed in many commercial cloud environments which have a cost per delivery. Location data (such as GPS) is an example of data which creates enormous potential value but is available to anyone with a GPS receiver.

8.3.3 SERVICES BASED ON DATA AVAILABLE FOR A COMMERCIAL FEE

Many companies see themselves as data delivery companies. Thomson Reuters, Bloomberg and Dow Jones will sell news, market announcements and financial market data to any buyer, with prices based on breadth of financial instruments, timeliness of data (real-time, near real-time, or historical data) and other quality factors. Companies can sell data without limit, and the data is used by regulators, hedge funds, algorithmic traders, and researchers.

23. See Fuel Check https://fuelcheck.nsw.gov.au/app (Accessed 6 August 2017).

Data In The Real World

In Australia, Equifax[24] has a product offering which includes the provision of credit reports for individuals and businesses. Equifax's data includes credit information on millions of individuals and commercial entities in Australia and New Zealand.

Australian company MARQ Services[25] provides an independent risk assessment for the Australian mortgage loan funding markets based on a set of data requirements with clear definitions, specifying a comprehensive set of risk and other loan-level information for mortgages. Their data requirements cover characteristics of the borrower, characteristics of the security property, terms and conditions and performance of the loan, and other information, such as the originator of the loan.

8.3.4 SERVICES BASED ON DATA AVAILABLE TO SELECTED OR QUALIFIED USERS

A very substantial change in access control occurs when it is not openly available even to those with the means to purchase it. Data which is only available to qualified or classified users include data released to research partners, to a formal consortium, or to people willing to accept non-disclosure terms.

In Australia, innovative companies such as Quantium and Data Republic have created ecosystems of data sharing which include banks, airlines, insurance, entertainment, grocery stores and many others. The data is shared at fine-grained level in very tightly controlled, trusted environments to ensure privacy is protected.

8.3.5 SERVICES BASED ON DATA WHICH CANNOT BE SHARED WITHOUT ANONYMISATION

Some data is considered so significant that it can only be shared in an anonymised form, and even then, only within a selected environment.

As mentioned above, in a recent controversial example, on 1 August 2016, the Commonwealth Department of Health released approximately 1 billion lines of de identified historical health data relating to approximately 3 million Australians. The information released included details on services provided to Australians by doctors, pathologists, diagnostic imaging, and allied health professionals together with details of subsidised scripts. It was expected that research institutions, health professionals, and universities would create valuable insights from the linkable, individual Medicare and PBS claims data for a random 10% sample of Australians. The data release included historical Medicare data (from 1984) and PBS data (from 2003) up to 2015.

24. See company website for further information http://www.equifax.com.au/
25. See company website for further information http://www.marqservices.com/about_us.html

To ensure that personal details could not be derived from this data, a suite of confidentiality measures, including encryption, perturbation and exclusion of rare events, was applied to the data. These safeguards attempted to ensure personal health information and individual patients and providers could not be re-identified. This data was quickly withdrawn from public availability after a research team showed they could identify a single (an 'any' anyone) in the data set.

09

A Two-Dimensional Framework for Services

Taking the two axes of Personal Information Factor and access control, it is now possible to describe service types within this simple framework. Figure 21 places example services within the two dimensions.

As discussed in Section 5.1, 'value' is a many factored issue associated with business impact, cost, and consequences of loss of exclusivity. The 'accessible' axis uses cost as a proxy for value with highly accessible data being considered low value, data that would be supplied for a nominal or commercial fee reflecting higher commercial value, and data which can only be shared under restricted conditions being highest value for which monetary compensation is insufficient consideration.

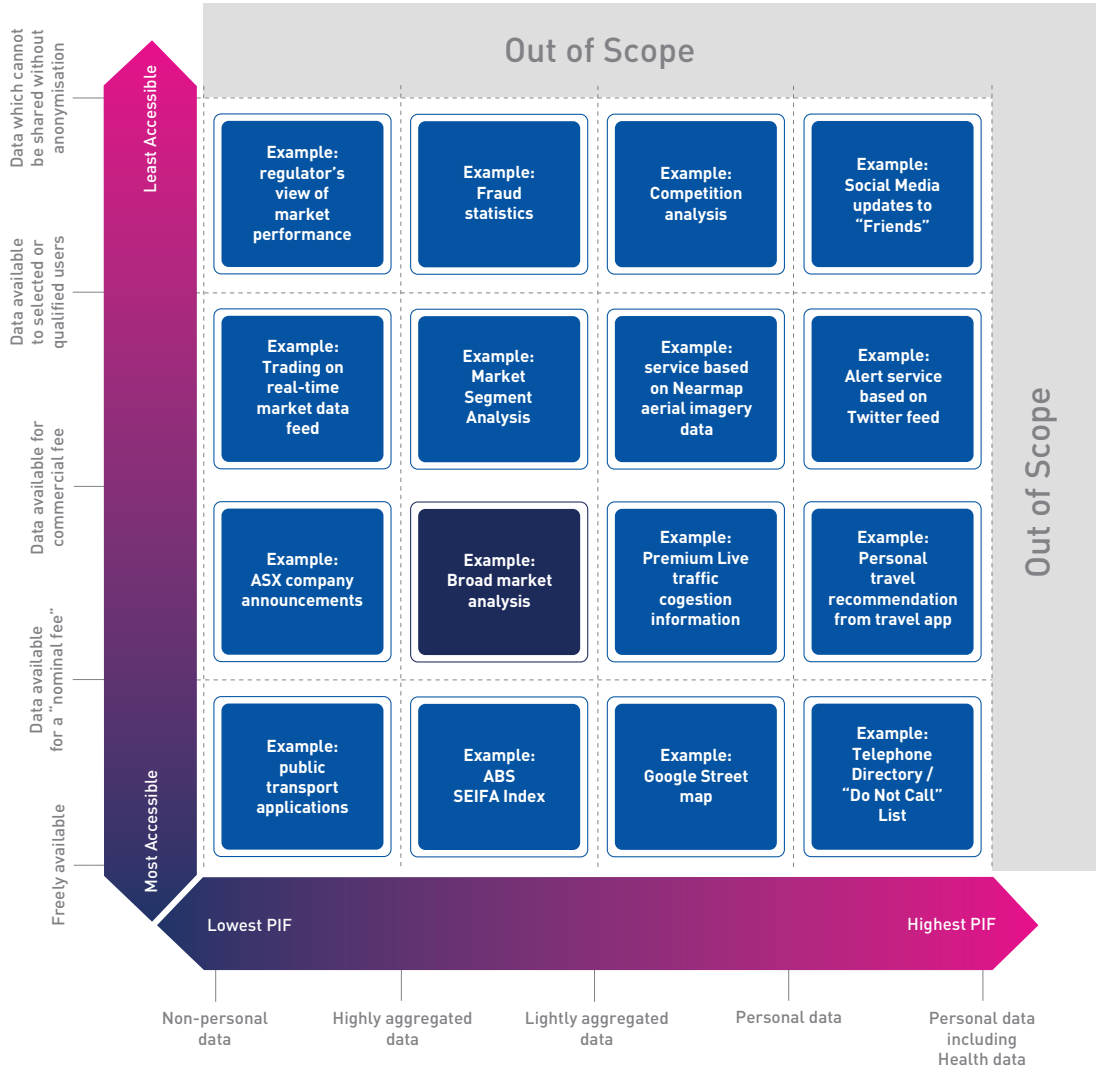


Figure 21. Service types according to persona information factor (PIF) and access

Perhaps surprisingly, many services exist based on data sets that contain clearly personal information. The extremely widespread use of social media tools means that by monitoring sources such as Twitter, it's possible to identify major events before mainstream media or government agencies. Twitter has been involved in the early detection of earthquake[26], fires[27] and other natural disasters alerting other Twitter users of events before government agencies or mass media even become aware.

In other cases, users share personal information in order to obtain a personalised service. In the case of a specific travel application, a user may be asked to allow access to the device's location (via GPS or other mechanism). Even if this access is denied, the device can gather personal information from origin destination pairs fed into the search process. At the very least, these are origin / destination pairs of interest. They may however reflect a journey that the user is about to undertake.

The frequent Facebook update is an example of highly personal information being shared within a trusted group. Whilst the user of the application may consent to data sharing, the individual members within a group photo, or bystanders, may not have the opportunity to consent (or be aware of an update). The context, membership, and environment of a group photo update all potentially contain highly personal information and so a high Personal Information Factor.

26. See, for example, early detection of 2014 earthquake http://www.dailymail.co.uk/sciencetech/article-2629991/earthquake-Twitter-beats-government-sensors-reporting-seismic-shocks.html (Accessed 6 August 2017).

27. See, for example, FAAST fire detection from Honeywell https://twitter.com/faast_detection (Accessed 6 August 2017).

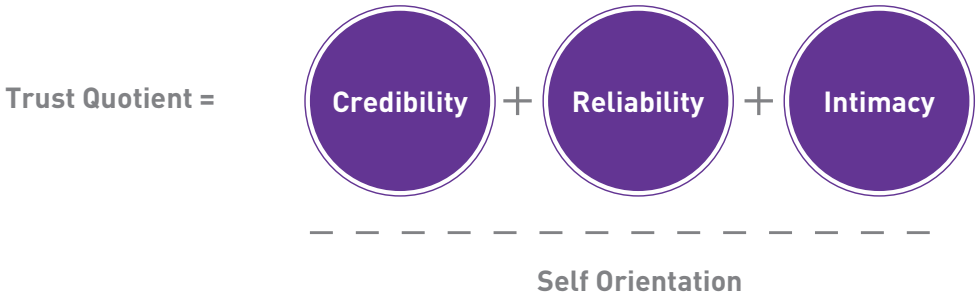
10

A Framework for 'Trust'

Trust is one of the most essential aspects associated with willingness to share data. People often are unwilling to share data in environments of low trust. Concerns are typically based on fear of unintended consequences, concerns about loss of control, loss of economic value, or concerns about adverse outcomes. Context is also very important when considering trust, what level of trust is required in different circumstances.

10.1 HOW DO YOU MEASURE TRUST?

Much of the challenge of data sharing is essentially related to trust. In this section, Trust is considered to be between the data source and the data recipient.



Credibility: Refers to the professional or technical credibility of the subject.

Reliability: Refers to actions and consistency of performance.

Intimacy: Refers to the safety or security that someone feels when entrusting the subject with important information.

Self-Orientation: Refers to the subject's focus and motivations.

Figure 22. The Trust Equation

In 2001, a heuristic model of trust was developed[28] to describe the major components of trust and how the challenges of developing a trusted relationship could be addressed. The Trust Equation described uses four objective variables to measure trustworthiness best described as: Credibility, Reliability, Intimacy, and Self-Orientation.

28. The Trusted Advisor, David H. Maister, Charles H. Green, Robert M. Galford, Andrea P. Howe, October 2001

The Trust equation provides a framework for potential interventions to improve the effectiveness of an engagement between individuals, or between an individual and an organisation.

The framing questions are:

- Can trust be measured?
- What is the role of context in trust?
- If trust can be measured, what are the units of trust?

10.2 THE UNITS OF TRUST

Information has been described in this paper in terms of the inverse of the probability of an event occurring out of a set of possible events. The less likely an event is to occur, the more information it carries.

Whilst this is only strictly true in closed systems with a finite set of possible events operating over a known channel, the principle has broad appeal when thinking of information as perceived by individuals. The more unexpected an event, the greater the 'information' associated with the occurrence of the event. News of an unexpected event in politics or international affairs carries a great deal of information[29].

Trust may be treated in a similar manner with the amount of trust associated with an event being the inverse the likelihood of an event occurring. The less likely an event is to occur, the more mistrust it carries. The number of mistrust 'bits' is then the logarithm (base 2) of the inverse of this probability.

Returning to the trust equation earlier in this section, it is worth testing to see how the analogy works in this framework. To assist with the framing, we will assume a time series based on units of time.

The analysis below assumes time invariant motivations and certain verifiable aspects of an engagement:

Credibility (C):
Refers to the professional or technical credibility of the subject. Assuming objective and verifiable measures of credibility (formal qualifications, professional associations, record of accomplishment) and that a person or source has not misrepresented themselves, then credibility will not change significantly over time.

Reliability (R): $R(t+1) = R(t) + 1$
Reliability refers to actions and consistency of performance. Assuming no unexpected events occur, reliability builds over time. We can postulate that reliability at time 't+1' is equal to the reliability at time 't' plus one.

29. The concept of 'information' in this context should not be conflated with 'interest'. News of events related to death, harm of children or unusual sexual conduct, rate highly on news and gossip channels, and are often labelled as shocking, scandalous or tragic. Whilst these events may carry information related to the probability of the event occurring, the higher profile the figures involved, the more likely they are to generate interest.

Intimacy (I): $I(t+1) = I(t) + 1 + Log_2(1/Prob(+ve\ Event(t))) - Log_2(1/Prob(-ve\ Event(t)))$

Intimacy refers to the safety or security that someone feels when entrusting the subject with important information. Intimacy builds over time and in response to 'Events' which occur over time. The equation above refers to the probability of an Event at time 't'. If the Event is positive, it increases intimacy. If negative, it decreases intimacy. If the Event has very low likelihood (probability close to zero, it is unexpected or 'shocking'), intimacy will be significantly affected. If the information shared has high probability (probability close to one, it is expected or not significant), it will have little impact on intimacy.

Self-Orientation (S):

Refers to the subject's focus and motivations. Assuming objective and verifiable measures of self-orientation (stated objectives, formal relationship, known intentions) and that a person or source has not misrepresented themselves, then self-orientation will not change significantly over time.

Whilst the analysis above is simplistic and necessarily requires strict assumptions (such as assuming time invariance and the need to determine positive and negative information), it provides some insights as to how trusted networks can be impacted.

Under these strong assumptions, the trust equation can be re-written as:

$$T(t+1) = (C(t+1) + R(t+1) + I(t+1)) / S(t+1)$$

$$= \frac{C(0) + R(t) + 1 + I(t) + 1 + Log_2(1/Prob(+ve\ Event(t))) - Log_2(1/Prob(-ve\ Event(t)))}{S(0)}$$

10.3 BUILDING TRUSTED NETWORKS

In October 2016, the US National Institute of Standards and Technology released a report[30] on development of trusted networks to support identity federations.

The NIST report describes trust frameworks in the following way:

A trust framework is developed by a community whose members have similar goals and perspectives. It defines the rights and responsibilities of that community's participants in the Identity Ecosystem; specifies the policies and standards specific to the community; and defines the community-specific processes and procedures that provide assurance. A trust framework considers the level of risk associated with the transaction types of its participants; for example, for regulated industries, it could incorporate the requirements particular to that industry. Different trust frameworks can exist within the Identity Ecosystem, and sets of participants can tailor trust frameworks to meet their particular needs. In order to be a part of the Identity Ecosystem, all trust frameworks must still meet the baseline standards established by the Identity Ecosystem Framework[31].

30. *Developing Trust Frameworks to Support Identity Federations - Internal Report 8149*, National Institute of Standards and Technology, October 2016, available online http://csrc.nist.gov/publications/drafts/nistir-8149/nistir_8149_draft.pdf
31. *National Strategy for Trusted Identities in Cyberspace – Enhancing Online Choice, Efficiency, Security, and Privacy*, April 2011

This statement speaks to:

- The need for participants to meet *baseline standards*
- The ability of participants to *tailor trust frameworks to meet their particular needs*
- The *level of risk associated with the transaction types*

Reframing this in terms of the trust equation, much can be done to improve the level of trust of stakeholders in a sharing system which more reasonably reflects real world situations:

- **Credibility** – ongoing and transparent evaluation of the performance of participants
- **Reliability** – ongoing and transparent evaluation of the sharing framework itself
- **Intimacy** – increase the level of choice participants have in selection of whom and what to share
- **Self-Orientation** – focus on removing perceived or actual self-interest (or misaligned interests) from the system.

10.4 THE NEED FOR RISK FRAMEWORKS

As discussed in Section 4, the risks of sharing data may be associated with potential loss of economic value, loss of exclusivity of data (data with personal information or of high strategic importance), or unintended consequences of the use of the shared data.

Taking the commercial value framework, there are a number of areas in which the use and access to data can be effectively evaluated. Figure 23 highlights these areas: cost of replacement, how data is currently being used in operational environments, how data is being used to drive key business outcomes, and how data contributes to company bottom line. Even if the economic value of this data remains elusive, the level of use and impact of not having access to the data can be estimated. As a consequence, a risk framework can be developed which addresses the risk of loss of access to this data.

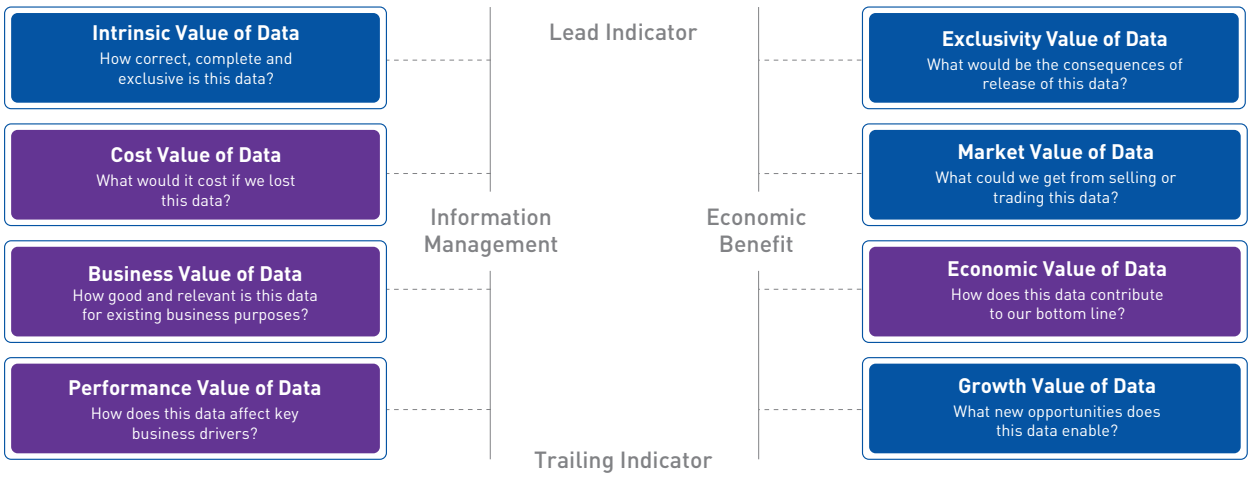


Figure 23. Areas where data value and use can be evaluated in a commercial environment

What is more challenging is to address the unknown opportunities or risks such as sharing data beyond intended users. Figure 24 shows the areas where the sharing of data must be estimated because they represent potential situations rather than existing environments. In the case of the potential loss of economic value, a financial consideration may be sufficient to compensate this risk. This may not be sufficient in the event of loss of exclusivity. Hence a different framework may be appropriate to address that risk.

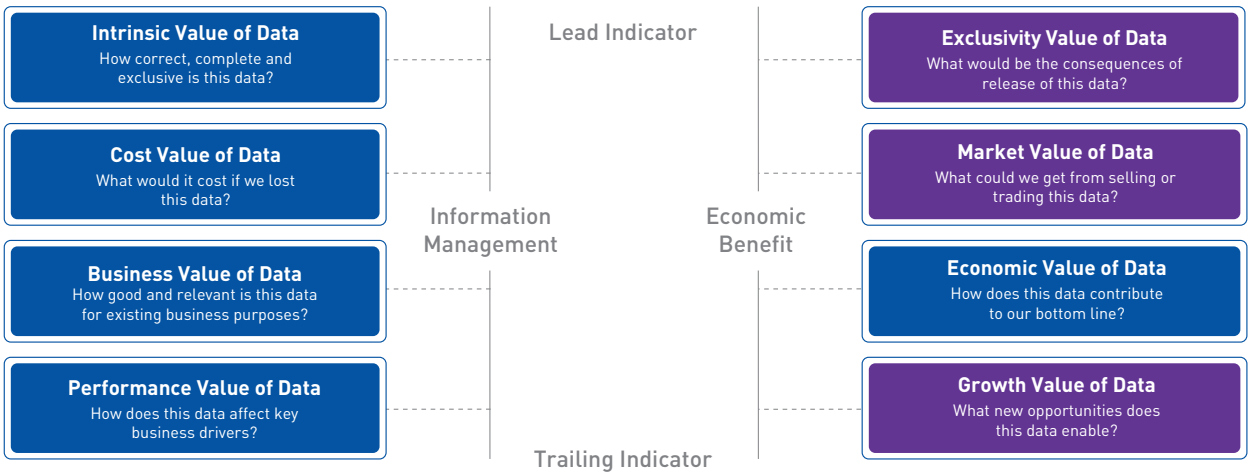


Figure 24. Areas where data value and use must be estimated in a commercial environment

The equivalent for government environments is shown in Figure 25. This figure includes the additional opportunity/risk of impact on the Research community as this is uncertain by its very nature.

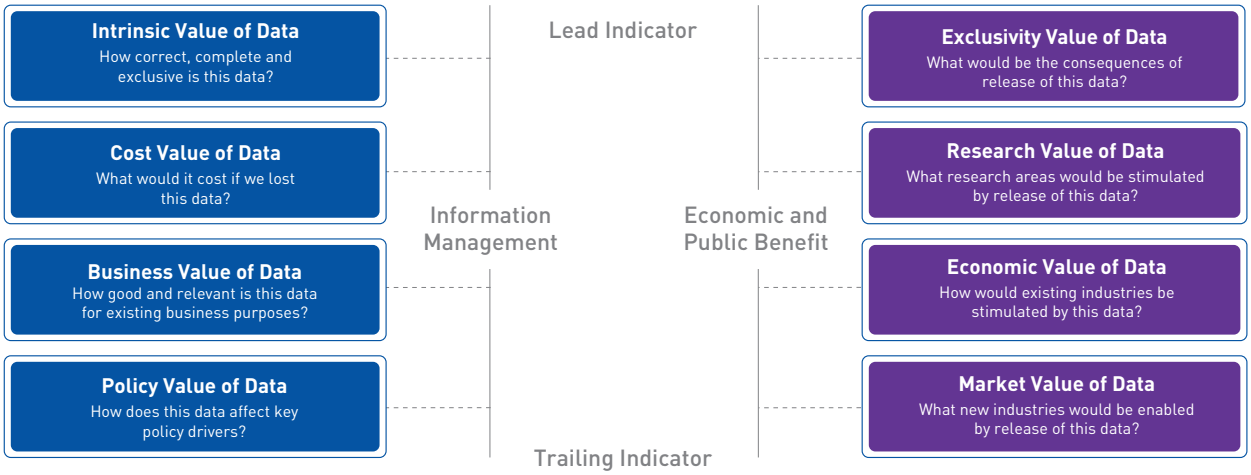


Figure 25. Areas where data value and use must be estimated in a government environment

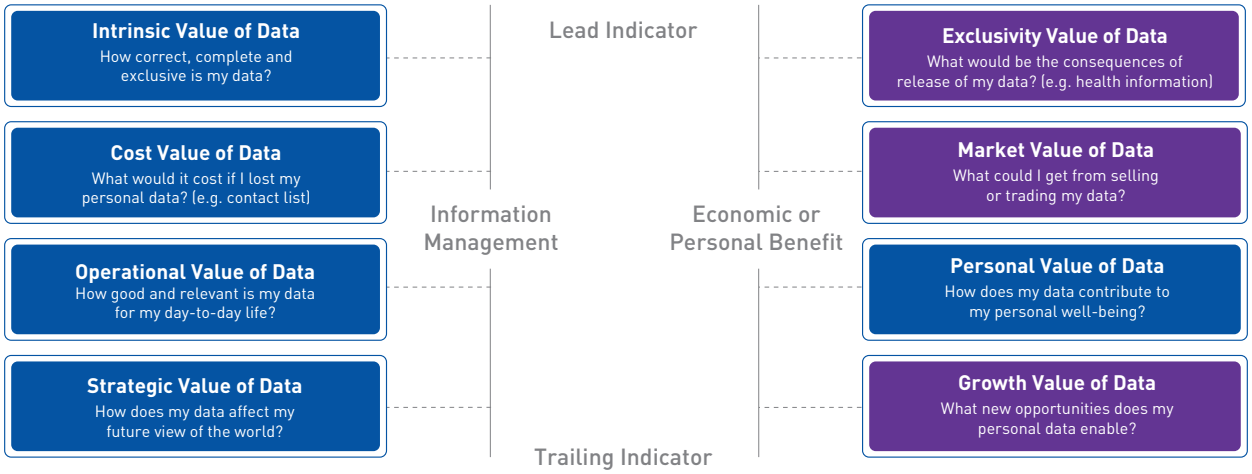


Figure 26. Areas where data value and use must be estimated for individuals

10.5 THE FIVE SAFES FRAMEWORK

A number of organisations around the world, including the Australian Bureau of Statistics, use a model referred to as the 'Five Safes'[32]. Originally developed by the UK Office of National Statistics, The Five Safes shown in Figure 27 is a framework for helping make decisions about making effective use of data which is confidential or sensitive. It was originally used to describe or design research access to statistical data held by government agencies, and by the UK Data Service.

Two of the Five Safes refer to statistical disclosure control (SDC), and so the Five Safes is usually used to contrast statistical and non-statistical controls when comparing data management options.

The Five Safes is a system framework. That is, it is intended to review how all the elements fit together. Taking the example above, the answer to whether a researcher is allowed to access a dataset assumes that all other necessary conditions are in place. Supposing secure facilities do not exist; then this does not seem like a good use of the data. However, this does not mean the questions of whether a researcher should have access to the data changes; only that the proposed solution as a whole is not acceptable – in this case because of a failure of the 'Safe Setting' dimension.

32. *Five Safes: designing data access for research*, T. Desai, F. Ritchie, R. Welpton, October 2016, http://www.nss.gov.au/nss/home.NSF/533222ebfd5ac03aca25711000044c9e/b691218a6fd3e55fca257af700076681/$FILE/The%20Five%20Safes%20Framework.%20ABS.pdf

The components of the framework are:

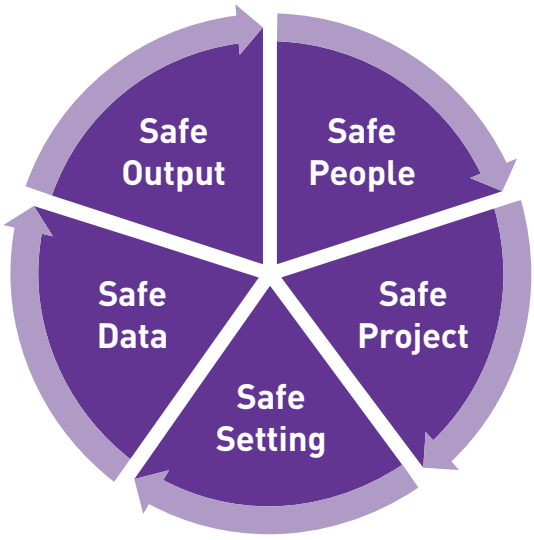


Figure 27. Five Safes Framework

Safe People
The knowledge, skills and incentives of the users to store and use the data appropriately. In this context, 'appropriately' means 'in accordance with the required standards of behaviour', rather than level of statistical skill. In practice, a basic technical ability is often necessary to understand training or restrictions and avoid inadvertent breaches of confidentiality; an inability to analyse data may lead to frustration, and increases incentives to 'share' access with unauthorised people.

Safe Projects
The legal, moral and ethical considerations surrounding use of the data. This is often specified in regulations or legislation, typically allowing but limiting data use to some form of 'valid statistical purpose', and with appropriate 'public benefit'. 'Grey' areas might exist when 'exploitation of data' may be acceptable if an overall 'public good' is realised.

Safe Setting
The practical controls on the way the data is accessed. At one extreme researchers may be restricted to using the data in a supervised physical location. At the other extreme, there are no restrictions on data downloaded from the internet. Safe settings encompass both the physical environment (such as network access) but also procedural arrangements such as the supervision and auditing regimes.

Safe Data
The potential for identification in the data. It could also refer to the sensitivity of the data itself.

Safe Outputs
The residual risk in publications from sensitive data.

The Five Safes model is relatively easy to conceptualise when considering the extreme cases of 'extremely' safe, although it is not possible to unambiguously define what this is. An extremely safe environment may involve researchers who have had background checks, projects which have ethics approval, and rigorous vetting of outcomes. Best practice may be established for such frameworks, but none of these measures is possible to describe in unambiguous terms as they all involve judgement.

The framing questions to be considered include:

- Is it possible to determine 75%, 50% or 25% safe levels for aspects of the framework (see Figure 28)?
- Could a 100% safe state for people be described and combined with a 25% safe setting?

Quantifying theses states will remain a challenge for this Taskforce.

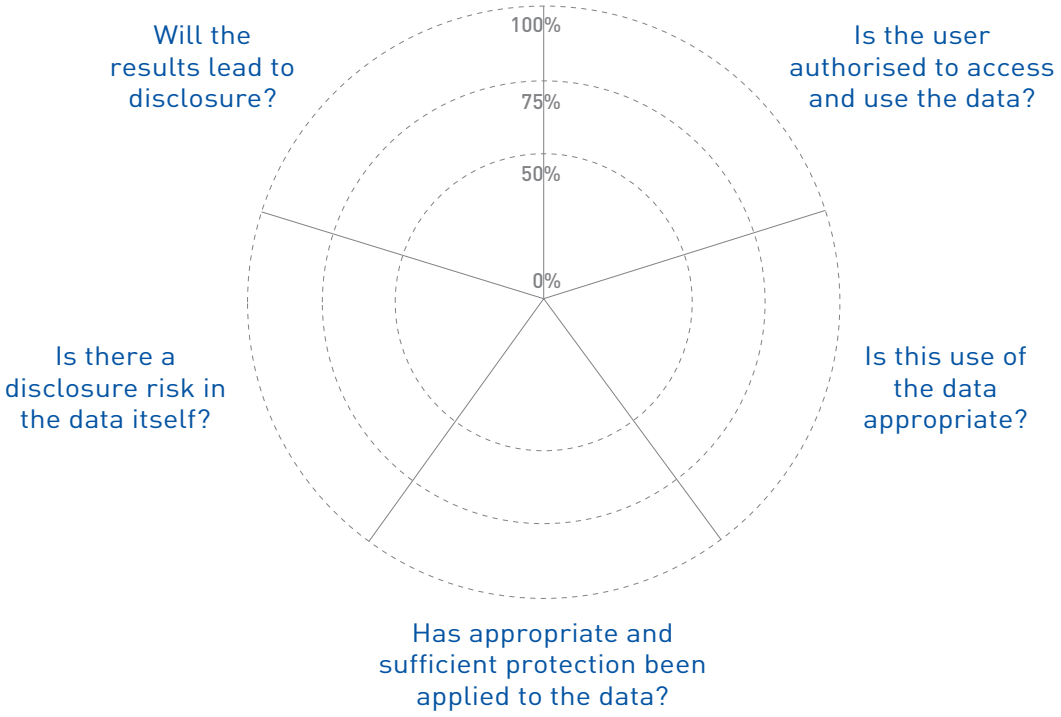


Figure 28. Quantifying in the Five Safes Framework

10.6 RISK OVER TIME

Similar to the discussion on value, an implicit assumption of data sharing is that risk decreases with the passing of time. In some countries, sensitive information and data associated national with security is released (declassified) after a specified number of years have passed.

In the United States, Executive Order 13526[33] establishes the mechanisms for declassifications. The originating agency assigns a declassification date, by default 10 years. After 25 years declassification review is automatic, with nine narrow exceptions that allow information to continue to be classified. At 50 years there are two exceptions, and classifications beyond 75 years require special permission.

33. See online https://www.archives.gov/isoo/policy-documents/cnsi-eo.html

But the question arises, it is necessarily the case that 'risk' of releasing data and the 'value' of data decrease over time? The answer to this is highly dependent on the use case and dependent on the information which is unlocked by access to the data.

For example, data associated with an individual may reveal details on personal health, habits, or preferences. As the individual's life progresses, the total data available on the individual increases and the potential for adverse outcomes increased.

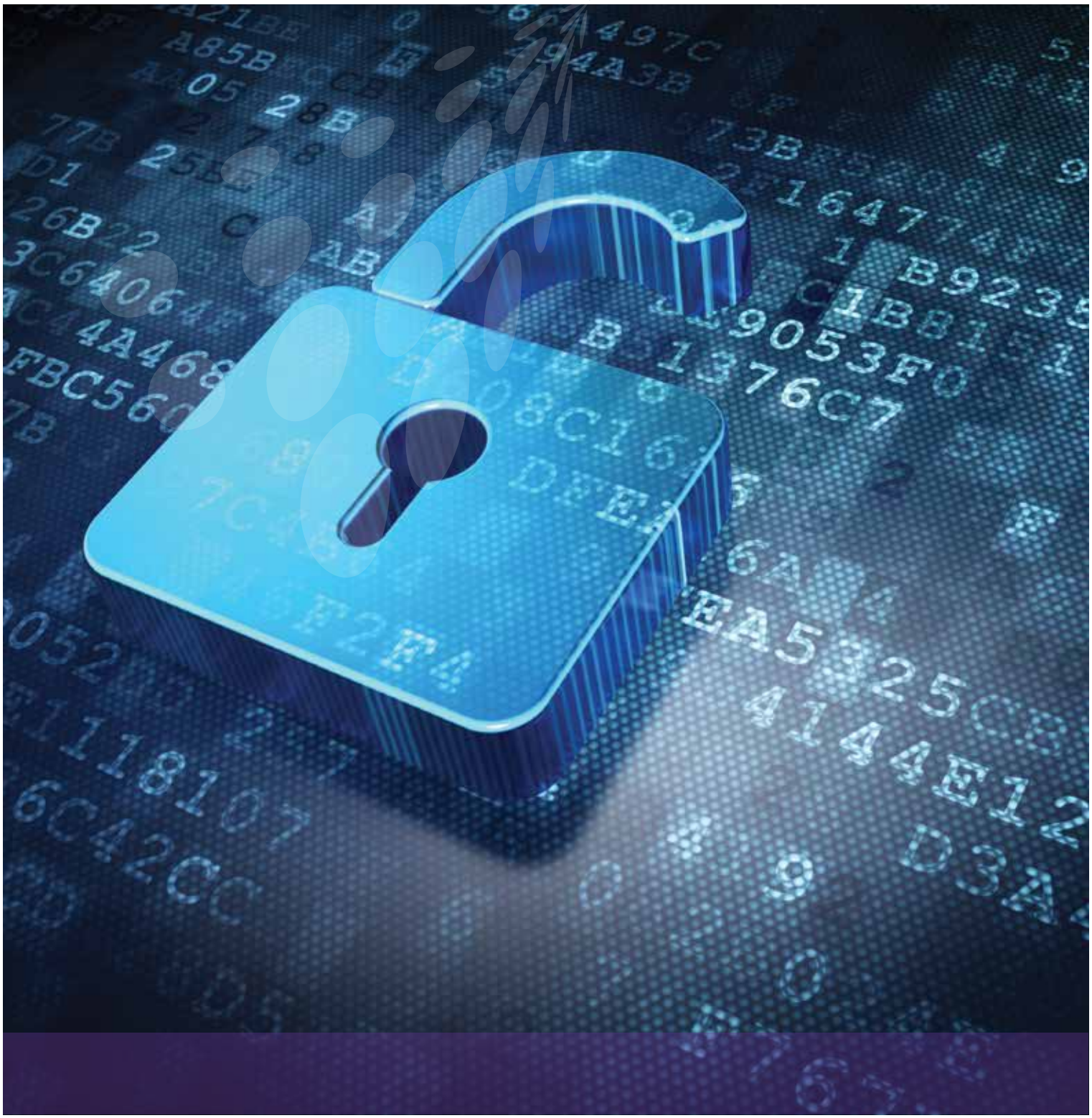
Data In The Real World

In July 2014, South African media reported that South African Broadcasting Corporation's (SABC) chair Ellen Tshabalala had misrepresented her qualifications. Tshabalala resigned from her position 6 months after the allegations first arose.

South African MP, Pallo Jordan was also exposed for faking qualifications when it was revealed that he did not have qualifications from the University of Wisconsin-Madison or the London School of Economics. Jordan resigned from his position as MP soon after he was exposed.

SA Airways Board Chairperson Dudu Myeni and Acting CEO, Nico Bezuidenhout were also accused of misinterpreting their qualifications. Myeni listed a Bachelor's degree in Administration as one of her qualifications when she was appointed in 2009 but the degree was ultimately removed from her CV in the company's annual report. She said she had listed the degree because she had been studying towards it. In two annual reports, Bezuidenhout was said to have a B.Com degree and an MBA which had never been studied for nor granted.

11



'Safe' Data Sharing Frameworks

The 'Five Safes' framework was developed for research projects and implies sharing of data in a controlled environment, performing analytical operations on the data, and then sharing the results of the analysis. For the purposes of the Data Sharing Taskforce, we can consider the simplest version of a project being simply passing through the data (no linkage or analytical work being performed), aggregating, or anonymising the data before sharing. Consequently, the Five Safes Framework will be examined in a data sharing context.

One of the implications that can be drawn from the discussion of the framework is that several of the dimensions are highly dependent on judgement. 'Safe People' and 'Safe Projects' are particularly dependent on a judgement-based evaluation of risk. Whilst frameworks may be developed to help decision making in these areas, there is no unambiguous way to determine quantified levels of 'safe' for these dimensions.

'Safe Setting' is largely depended on restrictions applied at a technology and governance level. This dimension will benefit from the exploration of 'A Frameworks for Reasonable' (Section 7), as well as the exploration of 'Anonymisation of Data' (Section 8.2). The aspects related to Governance will be dealt with in a later section.

The examination of the 'Safe Data' dimension will benefit from earlier sections which explored the 'Simple Data Sharing Framework' (Section 4).

The 'Safe Outputs' dimension brings us back to the heart of the data sharing frameworks challenge. The human context of recipients of the results of data analysis (data sharing) project, and the ability of any recipient to find additional data in the wider world combine with the outcomes of the data analysis project (Section 6). The examination of the 'Value of Data' (Section 5.) will be used to help frame this discussion.

11.1 EVALUATING SAFE PEOPLE AND SAFE PROJECTS

Evaluating Safe People requires an evaluation of intention, and judgement of the character of individual participants. This may be assisted by identification of conflicts of interest, reference checks, or specialised checks such as police checks, working with children checks or national security checks. The outcome of such an evaluation will then establish the level of access that can be provided to an individual participant, including the sensitivity of the data, and which sort of projects they may be involved in.

None of these checks provide a definitive indication of the intention of the person involved in the project, nor the likelihood that they will breach an aspect of the Safes model. Rather, identification of possible motive and evaluation of past performance are used as predictors of future actions.

Evaluating Safe Projects requires judgement of the purpose of the project from a risk and ethical perspective. Formally convened ethics committees exist in most countries to evaluate research projects and to provide guidelines for conduct when carrying out projects. As an example, the UK's Social and Economic Research Council (SERC) provides a framework for research ethics principles, procedures and minimum requirements[34].

34. Available online http://www.gla.ac.uk/media/media_326706_en.pdf

These minimum requirements include that:

- Research should be designed, reviewed and undertaken to ensure integrity, quality and transparency
- Research staff and participants must normally be informed fully about the purpose, methods and intended possible uses of the research, what their participation in the research entails ,and what risks, if any, are involved
- The confidentiality of information supplied by research participants and the anonymity of respondents must be respected
- Research participants must take part voluntarily, free from any coercion
- Harm to research participants must be avoided in all instances
- The independence of research must be clear, and any conflicts of interest or partiality must be explicit.

The SERC guidelines contain additional (non-exhaustive) considerations for research which involve:

- Vulnerable populations, for example, children and young people, those with a learning disability or cognitive impairment, or individuals in a dependent relationship
- Sensitive topics – for example participants' sexual behaviour, their illegal or political behaviour, their experience of violence, their abuse or exploitation, their mental health, or their gender or ethnic status
- Groups where permission of a gatekeeper is normally required for initial access to members such as children or the elderly
- Research conducted without participants' full and informed consent at the time the study is carried out
- Research involving access to records of personal or sensitive confidential information, including genetic or other biological information, concerning identifiable individuals
- Research which would or might induce psychological stress, anxiety or humiliation, or cause more than minimal pain
- Research involving intrusive interventions or data collection methods – for example, the administration of substances, vigorous physical exercise, or techniques such as hypnotism.

The SERC guidelines are typical of many ethical frameworks and require judgement from an expert panel in the event that issues are identified with the project.

Data In The Real World

On 20 April 2017, the National Health and Medical Research Council (NHMRC) released revised Ethical guidelines on the use of assisted reproductive technology in clinical practice and research (ART guidelines)[35]. The ART guidelines are used by professional organisations to set standards for the practice of ART. The ART guidelines are primarily intended for ART clinicians, clinic nurses, embryologists, counsellors and administrators, researchers, Human Research Ethics Committees, and governments.

When applied to the Five Safes framework, example threshold tests for Safe Project may include:

- **Assessed as 'Highly Safe'** – having no identified ethical aspects or not using data involving people
- **Assessed as 'Safe'** – having minor ethical risks which can be mitigated, or using highly aggregated or obfuscated data which has no residual personal information
- **Assessed as 'Moderately Safe'** – having ethical risks which require monitoring, or using lightly aggregated or obfuscated data with a possible risk of reidentification of individual information
- **Assessed as 'Low Level of Safety'** – having identifiable ethical risks which require significant attention, or using lightly aggregated or obfuscated data with a plausible risk of reidentification of individual information
- **Assessed as 'Not Safe'** – having clear ethical risks, or using personal information.

Under special circumstances, a project which is identified as having a Low Level of Safety or Not Safe on the scale provided above may still proceed if the public interest is perceived to be high. The level of governance required will be very high for these projects.

11.2 EVALUATING SAFE SETTINGS

Considering the Safe Setting dimension, the simple data sharing framework described in Figure 2 can be used to create a framework for providing access to data. The Safe Setting level implies that an assessment has already been performed for Safe People and Safe Project, as highlighted in Figure 29.

35. Available online https://www.nhmrc.gov.au/guidelines-publications/e79

As an example, threshold tests for Safe Settings assessed as Not Safe through to Highly Safe may include:

- **Not Safe** – system with no restriction on who can access data with ability to on-share
- **Low Level of Safety** – system with named user login authentication, limited ability to on-share
- **Moderately Safe** – system with multi-factor user authentication, no ability to readily on-share
- **Safe** – system with multi-factor user authentication, user action logging, prevention of on-sharing
- **Highly Safe** – system with multi-factor user authentication, active action logging, full audit trail of data lifecycle, anomaly detection, prevention of on-sharing.

Example settings which could be provided for People/Projects assessed as Not Safe through to Highly Safe may include:

- **Assessed as Not Safe** – provide access to open data only
- **Assessed as Low Level of Safety** – provide the ability to run defined sets of queries against highly obfuscated, perturbed, or aggregated data
- **Assessed as Moderately Safe** – provide the ability to run a wide range of queries against lightly obfuscated, perturbed, or aggregated data
- **Assessed as Safe** – provide access to lightly obfuscated, perturbed, or aggregated data
- **Assessed as Highly Safe** – whilst this will be dependent on situation, it may include providing direct unrestricted access to unit record data.

Data which is accessed in obfuscated or perturbed form will rely on technology as described in Section 8.2 or privacy preserving technology which will be discussed in a later section.

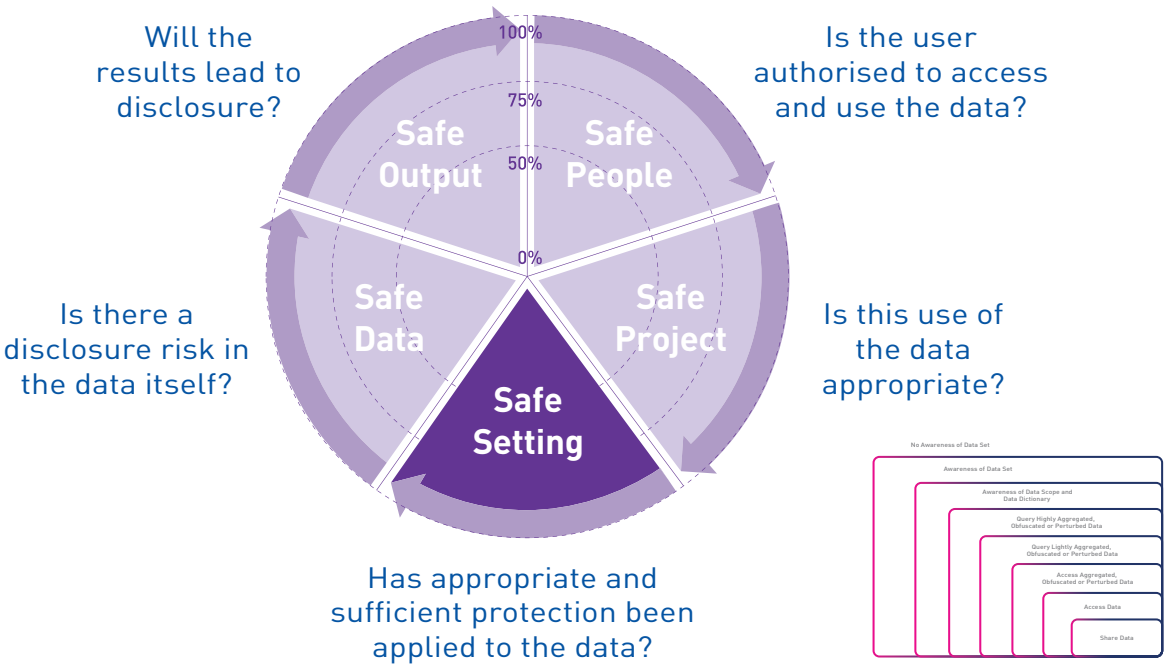


Figure 29. Data sharing frameworks with quantified access control

An important question to ask is how safe a setting is needed for different levels of Safe People and Safe Projects? What is the appropriate setting for a 'Safe Person' working on a project which is considered to have a Low Level of Safety?

Conversely, what level of access is appropriate to allow a person judged to be a Low Level of Safety to operate on a project judged to be Safe?

Figure 30 shows an example of how Safe Settings may be established for combinations of different levels of safety for People and Projects. This example relies on the Data Sharing Framework described in Figure 2 and technology-enabled governance. In this example, People considered to be 'Unsafe' (or unevaluated) only gain access to data which is publicly available. If open data is the only data used, it is impossible to overlay governance on a project. Projects which are evaluated as Not Safe are excluded from this example as they require individual evaluation.

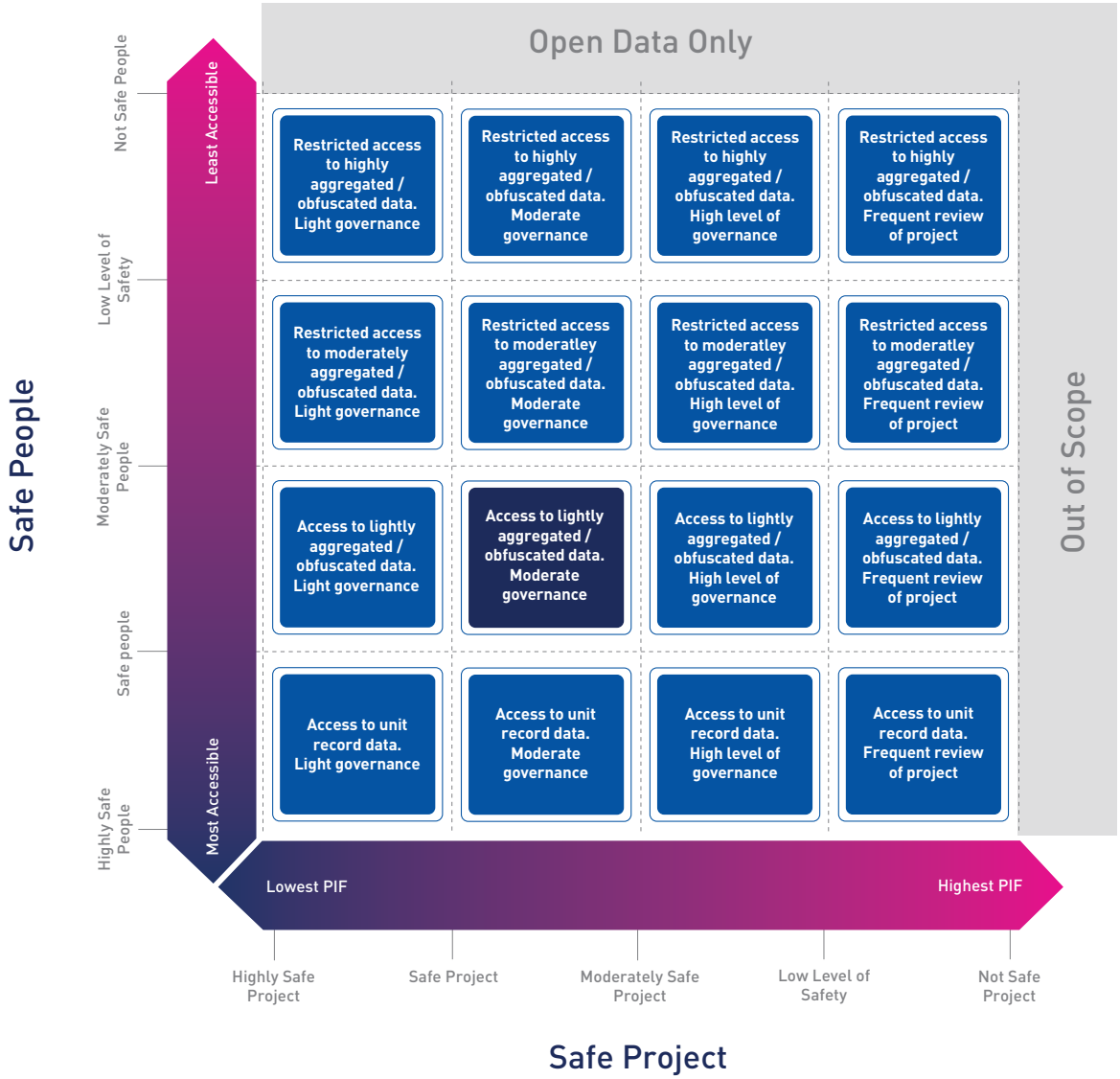


Figure 30. Safe Settings for a combination of 'Projects' and 'People'

Whilst technology cannot be considered to be the complete answer to Safe Setting, it can help mitigate risks for different levels of 'Safe'. Examples of systems which provide Safe Setting at different levels already exist. The challenge with many of these current frameworks is that they are not particularly well-suited to widespread, automated data sharing.

As an example, the SURE framework is a long-established framework which enables a researcher to access sensitive data. Authorised researchers working on approved projects operate on data within a constrained environment. Researchers can perform operations over unit record level data and cannot on-share data. Whilst addressing the needs of individual researchers, the system is not well-suited to wide ranging collaboration in its current form.

At the other extreme, systems such as data.gov.au provide examples of data sharing mechanisms for open data. While appropriate for the release of raw data, particularly from government agencies, it remains limited from the perspective of wide-ranging collaboration.

An area which is actively being developed is the technology which allows computational operations to be performed where the data is stored, and return the answer to a query (and not provide access to the underlying data). The anonymised computations can be distributed, performing calculations over multiple data sources, at multiple sites, and still returning just the computed outcome. These approaches are well-advanced, and while there will be a significant additional ICT burden associated with this approach, it may significantly lower privacy and legal concerns associated with use of data, and so reduce governance requirements.

11.2.1 HOMOMORPHIC ENCRYPTION

Perhaps the most interesting and exciting advancement in securing privacy in data analytics is known as *Homomorphic Encryption*. For more than 40 years, there have been public-key encryption systems that allow the user to perform simple arithmetic operations on numbers while they are encrypted, and to then decrypt the results.

As a simple example, consider the problem of determining the average salary of a group of people without any of them disclosing their individual salary. Using homomorphic encryption, each person can encrypt their salary, then all the encrypted salaries can be added together, and the result can be decrypted and divided by the number of participants, which will give the answer to the problem. No individual salary will be disclosed in the process as they are encrypted.

The principle is shown in Figure 31.

Figure 31. Homomorphic Encryption (*Source: Data61, CSIRO*)

To do this safely, it is necessary to keep sensitive encrypted information away from the party that can do the decryption. Secondly, it is important to consider any aspects which may be disclosive (higher Personal Information Factor).

For example, if there was a billionaire included in the set, the billionaire's data would dominate the result. Building systems that manage these risks is a significant part of the technology challenge.

Data In The Real World

In 2009 Craig Gentry at IBM[36] developed the first 'fully homomorphic' encryption system. These systems allow both addition and multiplication (and by extension, other arithmetic operations including subtraction and division) of encrypted numbers. This advance in capability is driving more and more innovations in this space and an ever-increasing adoption of these techniques into a range of applications.

36. For more information, see IBM http://researcher.ibm.com/researcher/view.php?person=us-cbgentry

11.3 EVALUATING SAFE DATA

The Safe Data dimension can be considered as a complementary to the Safe Setting dimension. If people or projects meet a certain threshold, then access can be given to ever more fine-grained data with lighter levels of obfuscation or perturbation. The challenge remains that, when linking data sets together, the risk exists of creating an unexpected insight which may lead to identification of personal information. This speaks to the challenge identified in Section 6.2 ('Is Personal Information Present in Data?'). This framework is illustrated in Figure 32.

The simple closed system framework described in Figure 7 can be used to conceptualise a framework for considering whether data is 'disclosive'. By scanning combinations of parameters in the data, a set of features can be identified which creates the smallest identifiable cohort. In this case, fully disclosive is taken to mean a cohort size of one, or having a PIF of one. Whilst identification of a cohort of size one is not always the same as being able to identify an individual, it is considered to be more likely to be able to identify an individual as the cohort size reduces.

As an example, the combined data sets of:

> *All males, born in Australia, in July*

Is less disclosive (lower PIF) than the combined data sets of:

> *All males, born in Sydney, Australia, in June of 1968, who live in Queensland and work for government, who have beards*

Whilst being able to identify how disclosive a data set is, the question is if the risk can be appropriately managed through governance (Safe Setting), limiting the scope of sharing of the data (Safe Output) or if the data must be perturbed to ensure a minimum cohort size is established.

Taking a cohort size approach, threshold tests for data may include:

- **Assessed as Not Safe** – data is anonymised but minimum cohort size is one
- **Assessed as Low Level of Safety** – data is anonymised and then obfuscated or perturbed resulting in a smallest cohort size of N *(N → 1)*
- **Assessed as Moderately Safe** – data is anonymised and then obfuscated or perturbed resulting in a smallest cohort size of M *(M → N → 1)*
- **Assessed as Safe** – data is anonymised and then obfuscated or perturbed resulting in a smallest cohort size of P *(P → M → N → 1)*
- **Assessed as Highly Safe** – data is anonymised and then obfuscated or perturbed resulting in a smallest cohort size of Q *(Q → P → M → N → 1)*.

The selection of minimum threshold values of N, M, P, and Q are deliberately avoided at this stage. Developing widely accepted threshold levels will be one of the recommendations of this Taskforce.

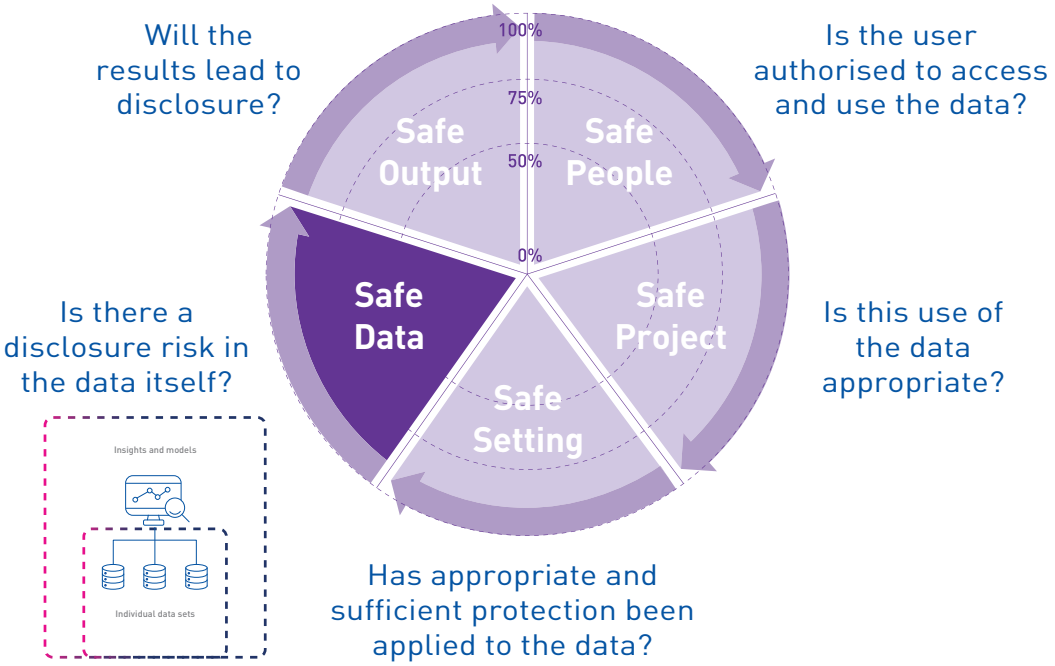


Figure 32. Data sharing frameworks with quantified Safe Data

11.3.1 PRIVACY PRESERVING LINKAGE

Another technology area showing promise relates to techniques to link databases together without revealing who is in the database.

These methods are based on 'hashing' functions – one way algorithms that when given two very similar inputs produce very dissimilar outputs, and do so in a way that it is not possible to deduce the inputs from the outputs[37]. These functions can be used to process personal information into 'keys' that allow matching of personal data between different databases.

Whilst the basic techniques for this have been known for many years, in the last 10 years, new methods have been established that allow matching between data even when the data has errors in it – such as spelling mistakes in names – while maintaining the required privacy guarantees. The principle is shown in Figure 33. This figure demonstrates 'fuzzy matching' in which the hashed version of names which are slightly different ('Kate Clark' and 'Kat Clark') can be matched with high probability based on examination of other factors.

37. For a discussion of different techniques, see for example, 'Privacy-Preserving Record Linkage', R. Hall and S. E. Fienberg, 2010, In: Domingo-Ferrer J., Magkos E. (eds) *Privacy in Statistical Databases*. PSD 2010. Lecture Notes in Computer Science, vol 6344. Springer. Available online https://www.cs.cmu.edu/~rjhall/linkage_survey_final.pdf

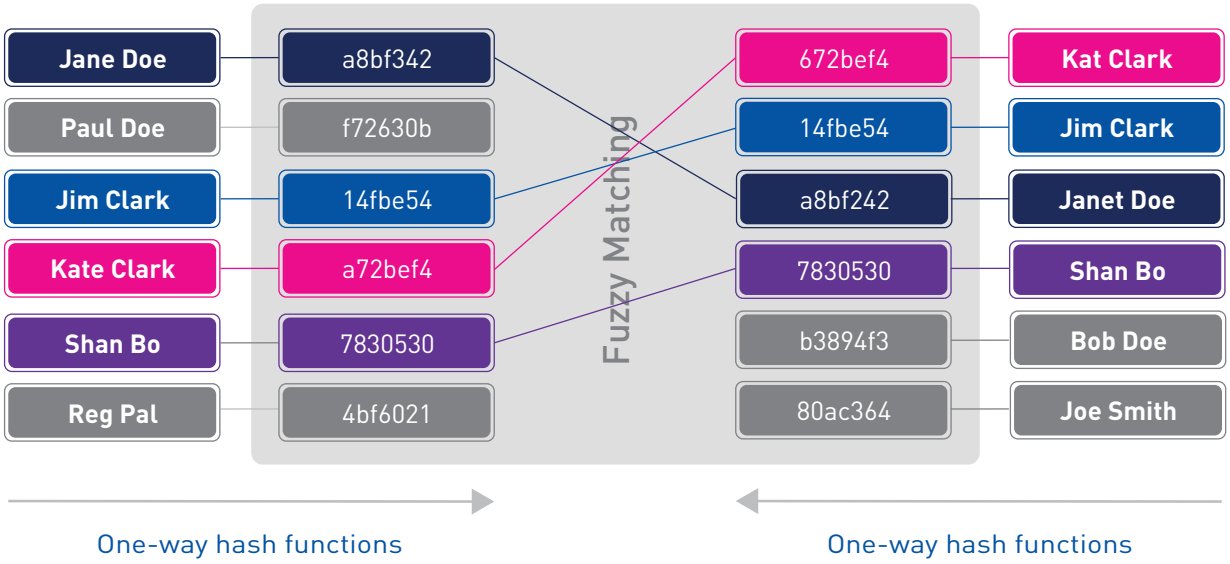


Figure 33. Private Record Linkage (*Source: Data61, CSIRO*)

These techniques of homomorphic encryption and privacy preserving linkage can be combined to enable a wide variety of analytics where the data, and the people the data is about, are hidden throughout the calculation. Record linkage enables data about different people to be lined up across different databases, and homomorphic encryption keeps the data itself secret. The principle is shown in Figure 34.

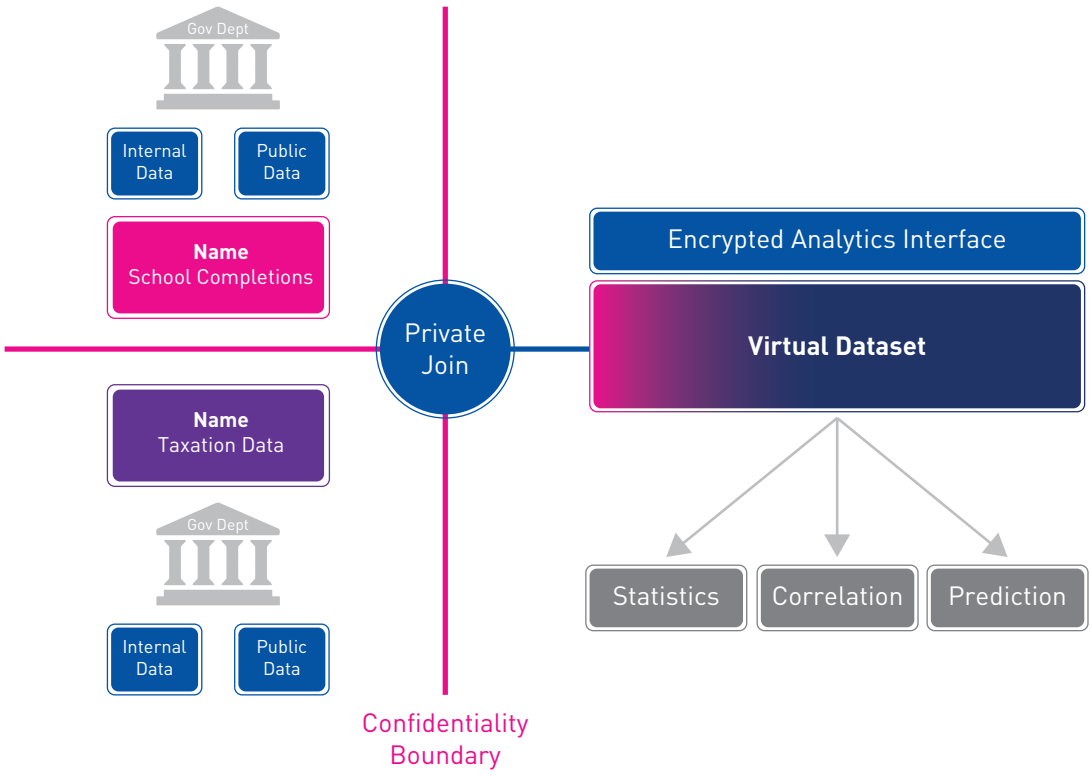


Figure 34. Confidential Computing (*Source: Data61, CSIRO*)

Applications include tasks such as the calculation of statistics across multiple databases held by multiple companies; as well as far more complex tasks such as the generation of predictive machine learning models across data from multiple organisations, all while keeping the data secret.

This technology space is moving rapidly, and has the potential to alleviate privacy and data security concerns in areas as diverse as health care to smart cities without disclosing our personal data.

These techniques also highlight new ethical concerns, as they enable applications that were not possible when they required the sharing of personal information.

11.4 EVALUATING SAFE OUTPUT

The concept of trusted sharing re-emerges as a major issue to determine if an outcome is 'Safe' to be shared.

The challenge of determining the level of safety remains the challenge of trusting that the recipient of a project outcome will use the knowledge as intended. This is complicated by the circumstances of the recipients as their knowledge and personal context may make the results more likely to disclose personal information. Added to this, a recipient's ability to find additional data in the wider world to combine with the outcomes of the data analysis project increases the potential for reidentification of an individual. The challenge again becomes one of risk management. The major factors of risk explored in this section relate to the value of the data and the level of safety of the project.

As an example, threshold tests for Safe Settings assessed as Not Safe through to Highly Safe may include:

- **Not Safe** – projects based on very high value data or projects which are considered Not Safe
- **Low Level of Safety** – projects based on high value data or projects which are considered to have a Low Level of Safety
- **Moderately Safe** – projects based on moderate value data or projects which are considered to have a Moderate Level of Safety
- **Safe** – projects based on low value data or projects which are considered to be Safe
- **Highly Safe** – projects based on open data or projects considered to be Highly Safe.

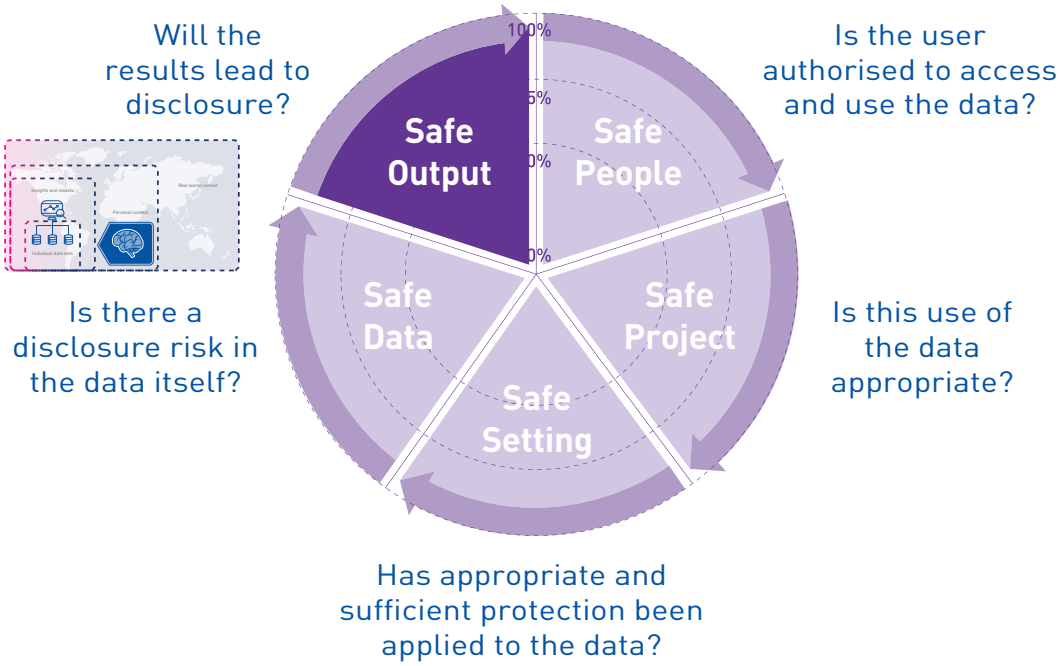


Figure 35. Data sharing frameworks with quantified Safe Output

For projects assessed as Not Safe to Highly Safe, a range of possible outcomes-sharing approaches can be applied.

Figure 36 shows an example of how 'Safe Outcomes' may be established for combinations of different level of safety for 'Project' and 'Data Value'. This example relies on the Value Framework described in Section 5. In this example, outcomes from Projects considered to have a 'Low Level of Safety', but which use data considered to be of low value, might share (anonymised) unit record outcomes but to named recipients. Unlike earlier sections, if open data is the only data used, it is still possible to limit access to outcomes as they are unique to the project.

Outcomes from projects using data which is evaluated as being 'Highly Valuable' are excluded from this example as they require individual evaluation.

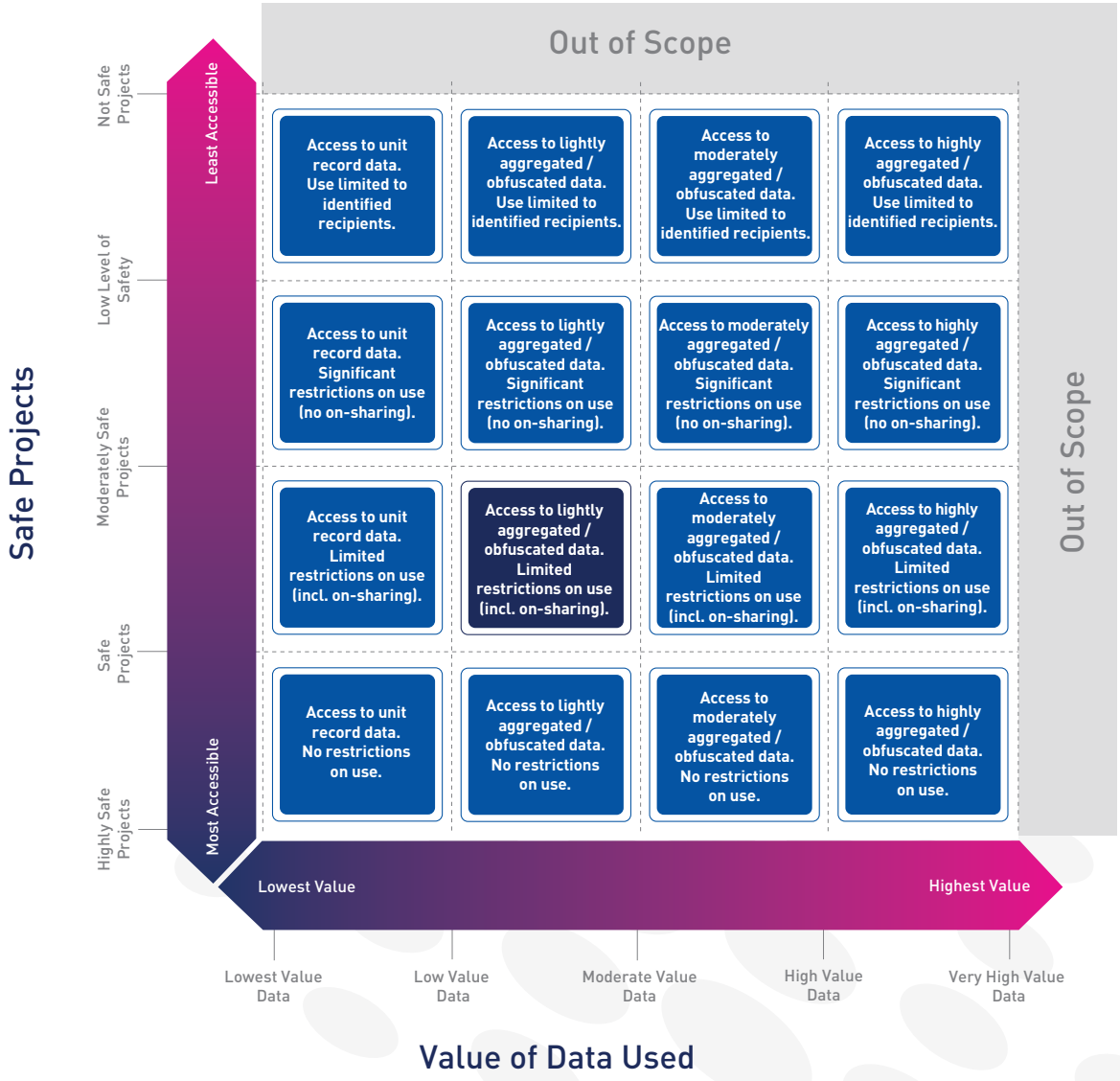


Figure 36. Example framework for Safe Outcomes for a combination of 'Projects' and 'Value of Data Used'

12

Governance Frameworks

Much of the discussion around data sharing has focused on trust and context. There is a strong requirement of trust within any data sharing agreement. Either the parties sharing the data must directly trust each other, or trust another entity whose job it is to protect each of the counterparties.

Technology can help to ensure that minimum thresholds are met or to control access, but ultimately the use of these tools and the appropriate handling of data is managed by a governance framework. Part of the role of a governance framework is to provide guidance to practitioners as to what to do, and then also the tools with which to do it.

With the discussion of the risk frameworks such as the 'Safe' Data Sharing frameworks in Section 11, it becomes clear that judgement of appropriate use or appropriate outcomes is required at multiple stages in the use of data: as a project is initiated, as data is gathered, as results are generated, and as results are released. In a project which involves an aspect of discovery, the conclusion that results for data to be 'Safe' to release cannot be made in most cases. Rather, an iterative review of 'Risk' is required at different stages.

The Framing questions for the Taskforce:

- What national standards or guidelines exist for data governance?
- Can we develop nationally accepted guidelines for different data types?
- Under what conditions can data with different levels of Personal Information Factor (PIF) be accessed, processed, and the results released?

12.1 EXISTING STANDARDS DRIVEN FRAMEWORKS

A standard protocol for defining requests and establishing data governance would improve the confidence and efficiency associated with data sharing projects, however the fundamental uncertainty as to the presence of personal information in sets of data sets highlights the limitations of most existing governance frameworks. The inability of human judgment to determine 'reasonable' likelihood of reidentification when faced with sets of large complex data limits the ability to appropriately apply the regulatory test.

12.1.1 ISO STANDARD 38505-1

In December 2015, Alison Holt published a framework for data sharing in the form of a Voluntary Code, based on the developing ISO standards for the Governance of Data[38]. The Code takes three areas from the data accountability map in the developing ISO standard 38505-1; namely Collect, Store, Distribute, and applies the aspects of Value, Risk and Constraint to provide seven maxims for sharing data. To assist with adoption and compliance, the Code provides references to best practice and examples.

38. Available online http://blogs.oii.ox.ac.uk/policy/new-voluntary-code-guidance-for-sharing-data-between-organisations/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+oiiblogs+%28Oxford+Internet+Institute+-+Blogs%29

With the release in 2017 of the ISO/IEC 38505-1:2017 standard, there are now internationally acknowledged guiding principles for the acceptable use of data within organisations. The standard is meant to apply to the governance of the current and future use of data that is created, collected, stored, or controlled by information technology systems, and impact the management processes and decisions relating to data.

The challenge with both the Voluntary Code and the ISO/IEC standard is that the basis is fundamentally Information Technology governance rather than the challenges explored by this Taskforce. The Code and the Standard do not explore 'value' as in Section 5, the framework for 'reasonable' as in Section 7, service types based on data usage as in Section 8, or a risk framework as discussed in Section 11. Consequently, more work remains to be done.

ISO/IEC 38505-1:2017

The ISO/IEC 38505-1:2017 standard provides guiding principles for members of governing bodies of organisations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of data within their organizations by:

- applying the governance principles and model of ISO/IEC 38500 to the governance of data
- assuring stakeholders that, if the principles and practices proposed by this document are followed, they can have confidence in the organisation's governance of data
- informing and guiding governing bodies in the use and protection of data in their organisation
- establishing a vocabulary for the governance of data.

ISO/IEC 38505-1:2017 can also provide guidance to a wider community, including:

- executive managers
- external businesses or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies
- internal and external service providers (including consultants)
- auditors.

While the standard focuses on the governance of data and its use within an organization, guidance on the effective and efficient governance of IT in its widest sense is found in ISO/IEC 38500 and ISO/IEC TR 38502. These documents look at the governance process at governing body level, principles for governance and, in ISO/IEC TR 38502, a framework and model for governance and the relationships between management and governance. Other documents in the 38500 family look at specific issues such as implementation, structure of principle based standards and governance of IT-enabled investments (in development).

12.1.2 EUROPEAN UNION – GENERAL DATA PROTECTION REGULATION

In April 2017, the Article 29 Working Party of the European Union (EU) published Guidelines on Data Protection Impact Assessment (DPIA)[39] in support of Article 35 of the EU's General Data Protection Regulation (GDPR).

39. Available online ec.europa.eu/newsroom/document.cfm?doc_id=44137 (Accessed 6 August 2017).

DPIAs determine whether processing is "likely to result in a high risk to the rights and freedoms of natural persons". A single DPIA may address either a single data processing operation or multiple processing operations if they are similar in terms of risk, scope, context, and purpose.

The GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. Performing a DPIA is only mandatory where processing is "likely to result in a high risk to the rights and freedoms of natural persons". The guidelines particularly highlight the need for a DPIA when new data processing technology is being introduced.

A summary of the guidelines and process are given in Figure 37 and Figure 38 respectively. It is worth nothing that the risk factors taken into account are broader than protection of personal privacy. Unlike many privacy regulating jurisdictions, the GDPR regulates 'profiling': that is, differential treatment of (possibly unidentified) individuals based upon inferences as to their characteristics or likely behaviour.

The GDPR distinguishes between what could be called 'common profiling', which involves analysing or predicting aspects of someone's life, and a narrower type of profiling that produces legal effects concerning an individual or significantly affects an individual. The second, a sub-set, is seen as 'high risk profiling' and is subject to specific rules under the GDPR, including a requirement of greater transparency, the right for affected individuals to challenge decisions, and an obligation to undertake a data protection impact assessment.

The penalties for non-compliance in fulfilling DPIA requirements are significant. Violations can result in fines of up to 10 million euros or up to 2% of the organization's total worldwide annual turnover for the preceding financial year.

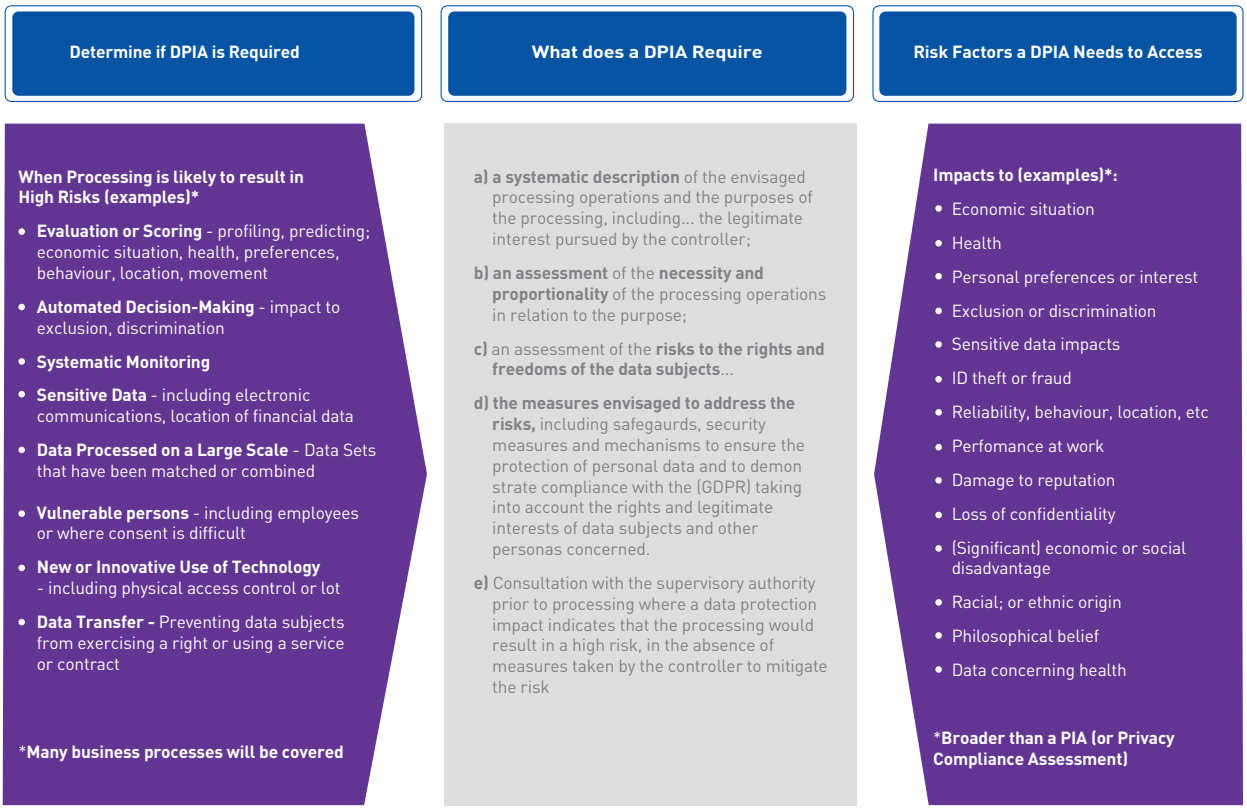


Figure 37. DIPA Requirements – When and What to Do

Other non-privacy concerns that might be considered include:

- The need to sustain citizen trust in processes of government, and to fairly and transparently use information collected in the public interest, often under regulatory compulsion upon the citizen to provide this information

- The commercial imperative for businesses to sustain consumer trust in order to ensure that individuals continue to deal with the business. Businesses have incentives (whether or not reflecting application of principles of corporate social responsibility) to use information gathered about consumers in the course of provision of products or services to them in a socially responsible manner – and in accordance with the consumers' reasonable expectations – having regard to the nature of the goods or services, and any pre-existing or ongoing business relationship between the consumer and the business

- Fairness, in the sense of expected cultural standards as to social equity

- Expectations of individual dignity, in the sense of expectations that individuals should be treated equally unless there is an ethical jurisdiction for distinctions to be drawn between individuals.

Where legitimate concerns as to fairness, ethics or trust may be anticipated from uses of 'outputs or outcomes' of data sharing or data analytics projects, and regardless of whether personal information will be used or disclosed in relevant outputs or outcomes, the degree of effect upon individuals, and the justifications for that effect, might be considered in an outputs and outcomes assessment, conducted by a reference group appropriately constituted to fairly consider and balance benefits and the above factors.

The constitution of such an output or outcome assessment reference group may be different from that used to conduct privacy impact assessments as privacy impact assessments generally have a narrower focus. For example, whilst a privacy impact assessment may evaluate whether relevant data linkage is through processes in a properly controlled and safeguarded data ecosystem, ensuring linked information is secure and properly de-identified, albeit not fully anonymised, and all outputs risk assessed as low or remote re-identification risk. Privacy impact assessments generally do not address unfairness or otherwise unacceptable effects upon individuals.

12.2 EVOLUTIONARY GOVERNANCE MODELS

One of the fundamental principles underpinning the challenge of data sharing is addressing the challenge of value, risk and trust in data sharing. This can change as a data analysis (the simplest case being data sharing) project develops through the major phases of:

- Project scoping (including identification of people)
- Data collection, organisation and curation
- Data analysis
- Results interpretation
- Release of results.

As each of these phases progresses, the 'value' of the outcomes increases, and the potential risk may also increase. The 'value' versus risk trajectory a project follows depends on the factors considered throughout this paper and may be mitigated by the approaches used in Section 11.

An important consideration is that projects which involve any element of discovery need periodic review depending on the level of risk which is assessed at each of the major project phases. Identification of the impact on privacy or the ethical considerations of a project will depend on what is identified – and this may not be known at the outset.

A more flexible approach to data analysis projects may allow light touch up-front assessment of privacy impact, people and technology, and increase the frequency or intensity of these assessments as the project continues.

A summary of possible guidelines is given in Figure 38. Figure 39 attempts to map the major data analysis project phases to the risk mitigation focus for each dimension in the Safes model. The benefit of a multistage assessment for privacy and ethics is that it is no longer necessary to preconceive at the outset of the project all of the issues or risks which may arise during analysis.

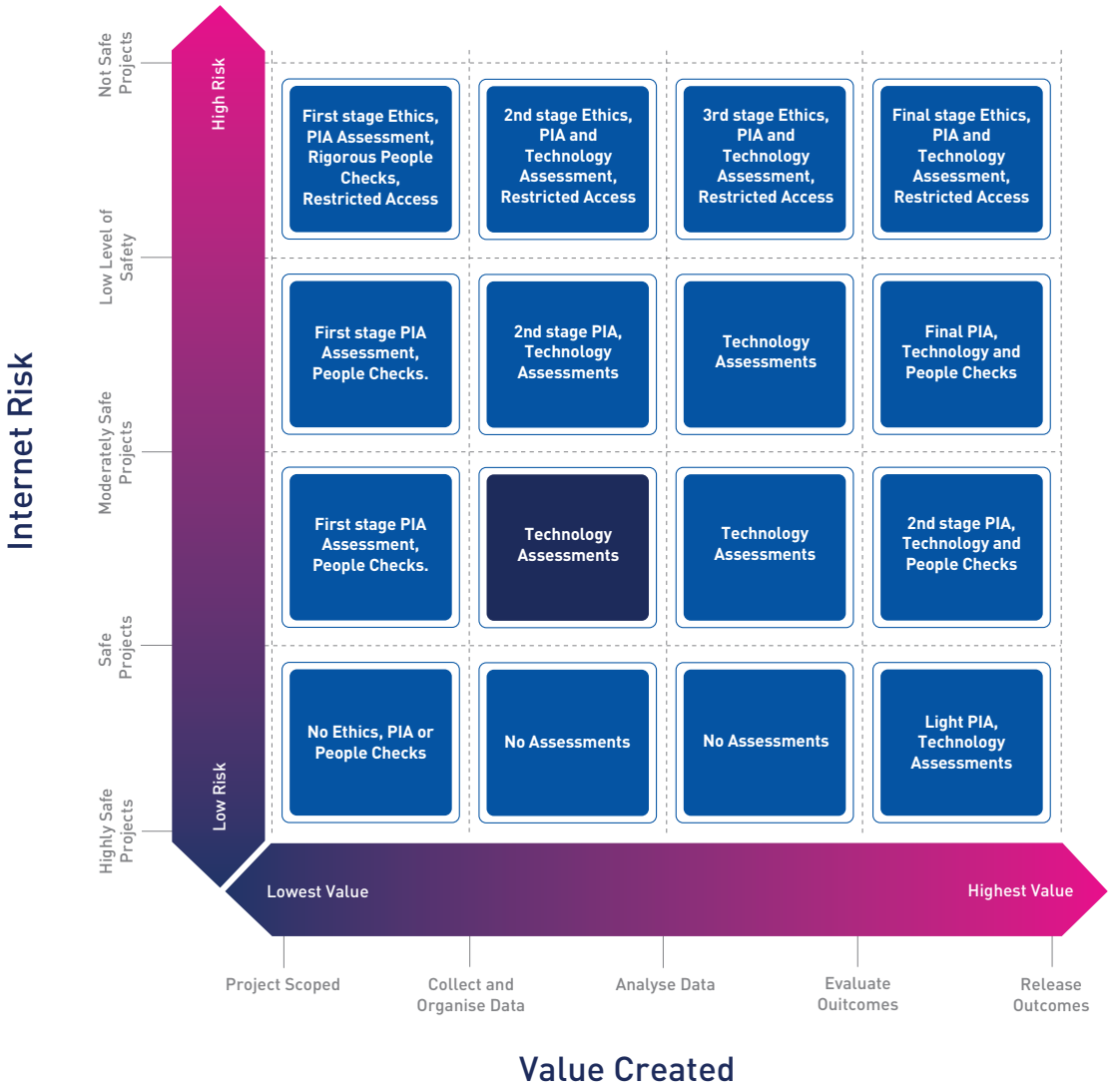


Figure 38. Ethics, Privacy Impact, Technology, and People assessments for different risk levels

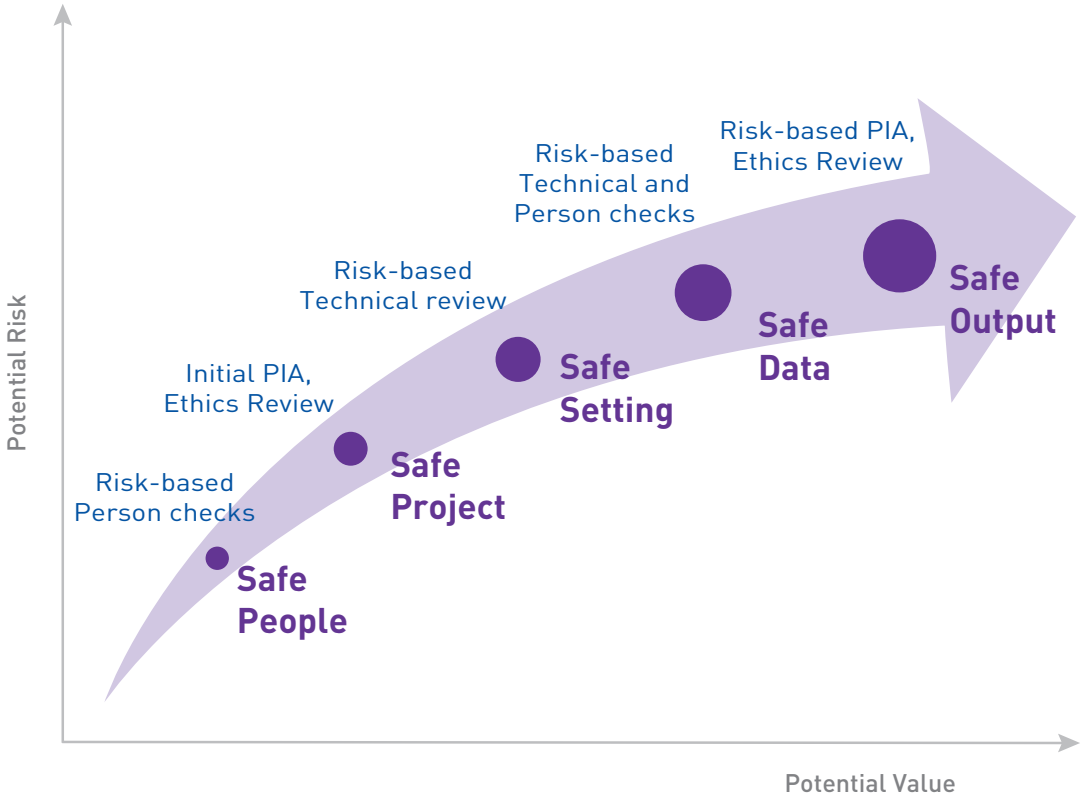
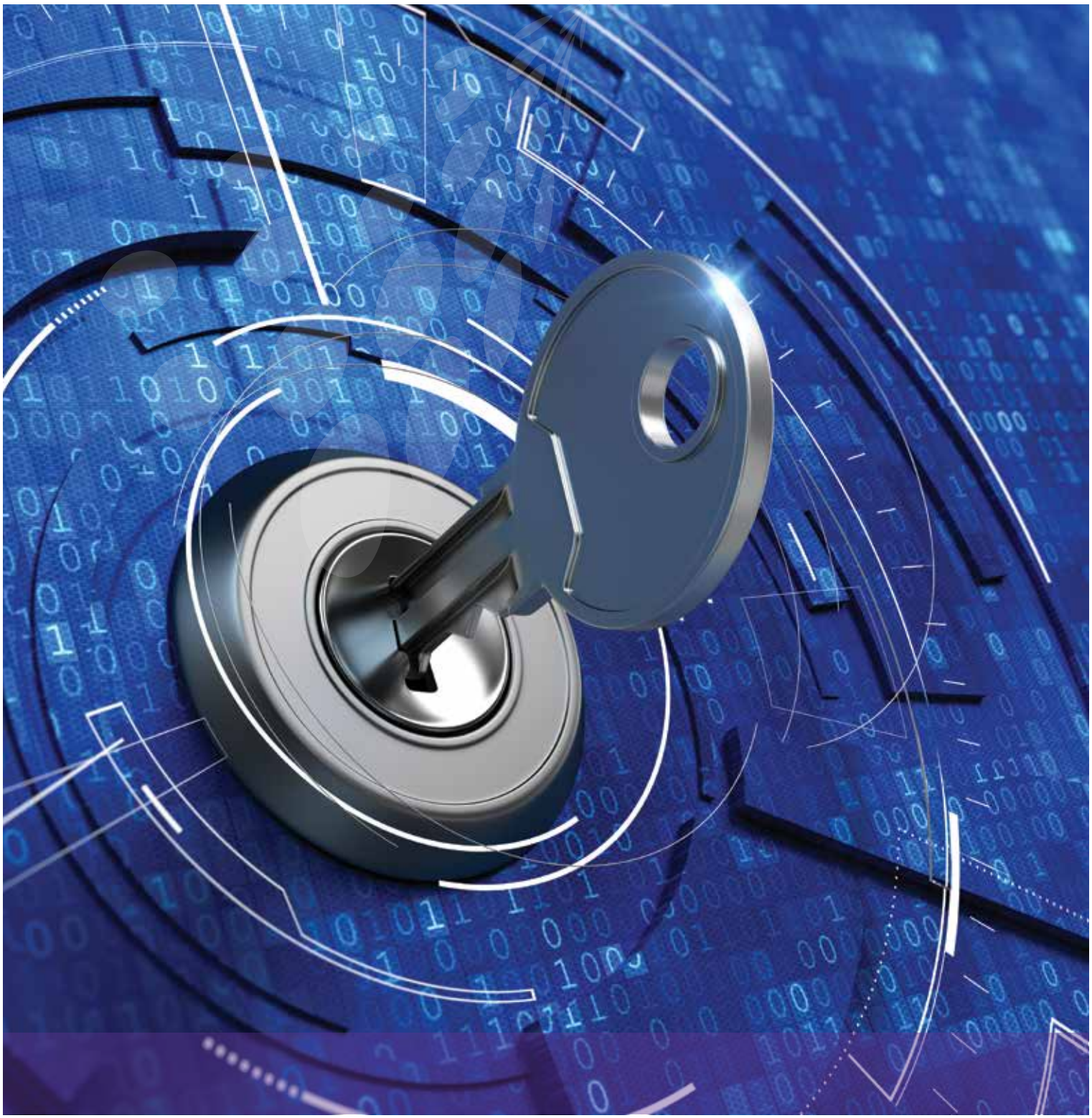


Figure 39. Mapping to the Five Safes Framework

13



Conclusions

Underpinning the transformation to a smarter, truly digital economy is the ability to share data beyond the boundaries of an organisation, company, or government agency. Future smart services for homes, factories, cities, and governments rely on sharing of data between individuals, organisations, and governments. The ability to create locally optimised, individually-personalised services depends on sharing of ever more personal information in the form of preferences, context, and usage patterns.

Beyond the technical challenges, data sharing comes with a range of legal obligations, privacy considerations, data security requirements, and concerns about unintended consequences of data sharing. These factors are highly dependent on the question of whether personal information is present in sets of data sets.

A fundamental challenge to answering this question is that there is no way to unambiguously determine if personal information is present in linked data. Even if an unambiguous test was possible for a given data set, the practical reality is also that data sharing does not occur in a vacuum. In almost any imaginable environment, aggregated data can be linked with data from other sources and so decomposed to a more personal level. The ability to increase the level of Personal Information Factor is limited only by the determination and ability to link extraneous data to the set which has been shared.

The ambiguity about the presence of personal information in sets of data sets highlights the limitations of most existing regulatory frameworks. The inability of human judgment to determine 'reasonable' likelihood of reidentification when faced with sets of large complex data limits the ability to appropriately apply the regulatory test. This ambiguity is the fundamental challenge being addressed by the goals described in Section 2.1.

Development of standards around what constitutes 'anonymised' would help to address the challenges of dealing with privacy. In all parts of the world, there is currently only very high-level guidance, and certainly nothing quantitative, as to what 'anonymised' means, hence many organisations must determine what 'anonymised' means to them based on different data sets.

Technology can potentially play a role to address this challenge but agreeing and then communicating what an acceptable degree of anonymisation is, and how to achieve it in quantitative terms, would also greatly improve data sharing. This clarification of existing legal frameworks needs to include quantified descriptions of acceptable levels of risk in ways which are meaningful for modern data analytics.

The technologies discussed in this document – determining minimum cohort size, differential privacy, homomorphic encryption, and privacy preserving linkage – all address concerns associated with re-identification of individuals from linked data sets. The space is moving rapidly, and has the potential to alleviate privacy and data security concerns in areas as diverse as healthcare to smart cities without disclosing our personal data.

The power of computational data analytics and the ability of new techniques to address expressed concerns about privacy actually surfaces a newer and bigger ethical concern. The privacy-preserving computational techniques enable applications that were not possible when privacy legislation was framed, and when the concept of privacy was considered in a joined-up digital economy. The unease that some privacy advocates feel about new personalised services is not readily addressed by the discussions of minimum cohort size or homomorphic encryption. The question that best describes these concerns: ***just because we can, should we?***

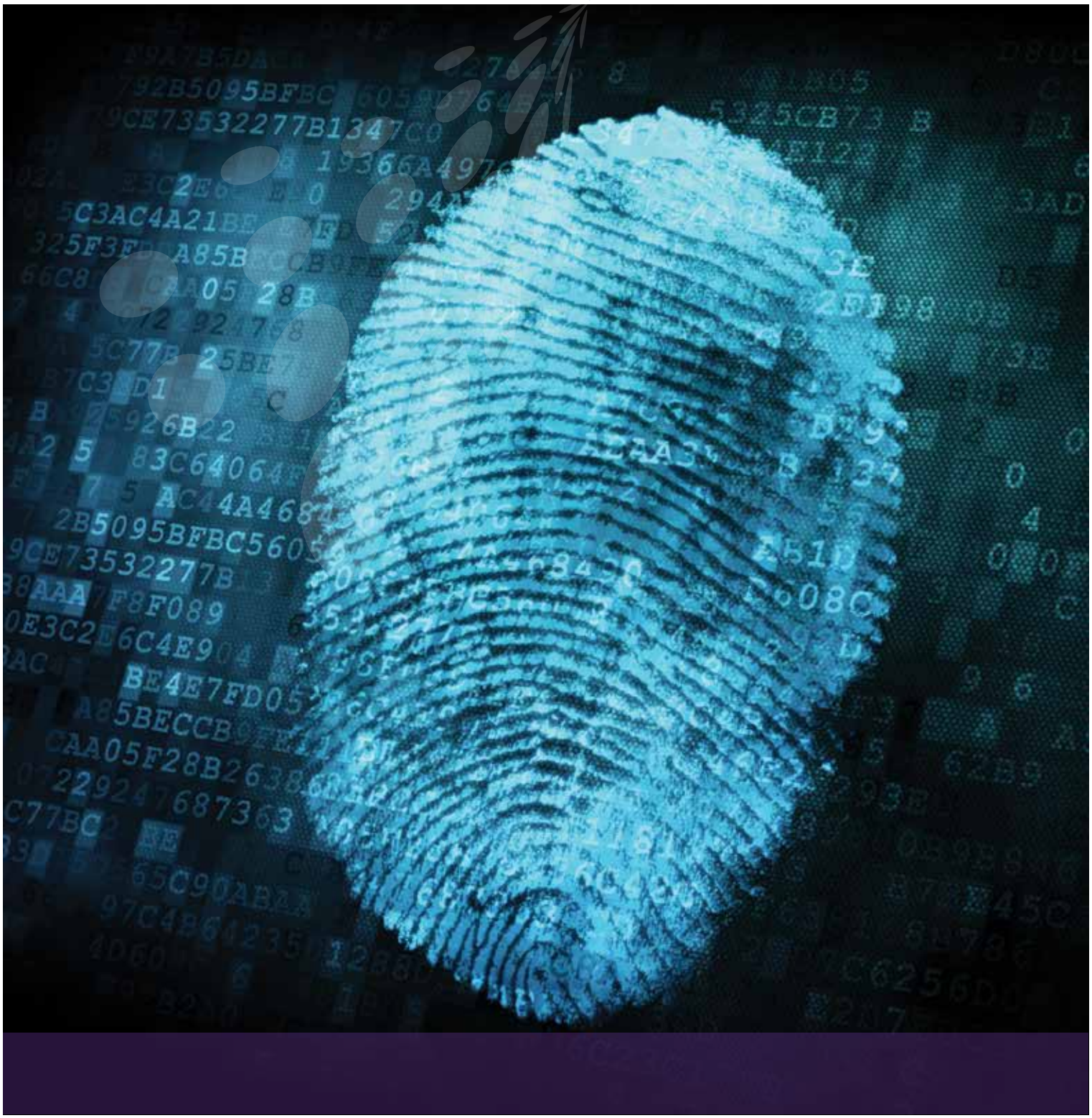
The irresistible digitisation of our lives coupled with innovative application of analytics have led to astonishing changes in the way we understand the world, the services we create, and the level of intimacy companies have with customers.

The challenge to address head on is identifying the sources of this unease at their most fundamental level, developing practical frameworks which allow the creation of value and yet preserve our privacy, and then adapting these frameworks for jurisdictions in Australia.

The higher order challenge is to reframe the national conversation on data sharing to be around the service created from data and the rights and obligations of people creating, delivering, and using these services.

The prize is the opportunity to create benefit for Australian industry, increased efficiency of government, and greater decision-making transparency for the citizens of Australia, while still protecting the rights and sensitive, personal information associated with each of us as individuals.

14



Recommendations

RECOMMENDATION 1:
Regulatory clarification

Regulatory complexity is one of the major challenges associated with greater sharing of data. It is far too easy to read 'not allowed' into existing regulations at one or more levels and so effectively prevent opening up of data.

The ambiguity about the presence of personal information in data sets highlights the limitations of most existing regulatory frameworks. The inability of human judgment to determine 'reasonable' likelihood of reidentification when faced with sets of large complex data limits the ability to appropriately apply the regulatory test.

Clarification of existing legal frameworks needs to include quantified descriptions of acceptable levels of risk in ways which are meaningful for modern data analytics, such as those described in this paper. Clarifying regulations associated with the release and use of data will help encourage industry and different government agencies to open up and share data.

RECOMMENDATION 2:
Development of a framework which supports anonymisation of data which in turn facilitates sharing

The areas which have the greatest potential to drive productivity in Australia are also the areas which require access to the most sensitive and personal data sets – health, superannuation, human services, and education. A focused effort on mechanisms which allow data to be anonymised and shared with industry and the research community will open up many of the biggest challenges facing Australia to the academic scrutiny and industry-led innovation.

New technologies – determining minimum cohort size, differential privacy, homomorphic encryption, and privacy-preserving linkage – all address concerns associated with re-identification of individuals from linked data sets, and yet all are at relatively early stages of development. Maturing these technologies by encouraging pilot projects and safe trials would benefit all jurisdictions.

RECOMMENDATION 3:
A test for Personally Identifiable Information – develop a nationally accepted test for the existence of Personally Identifiable Information

Information is created when data sets are joined. Collating data from millions of sensors operating at billions of cycles per second is fundamentally incompatible with relying on human judgements to determine the existence of personally identifiable information. Creating a nationally acceptable test will greatly increase the scope for smart services, whilst still leaving room for judgement in risky situations.

RECOMMENDATION 4:
Agreed standards for minimum cohort size based on data type

By its very nature, the concept that a cohort size of one *is always* the same as identification of an individual is an unprovable statement. Given the increasing variety of data available and accelerating analytical capability, it is however tempting to say that they are the same. In order to protect individual privacy and to acknowledge concerns about 'likely' or 'reasonably' reidentification, minimum cohort sizes should be agreed and communicated for different levels of data value. This would help data joining and minimise challenges around use of widely varying levels of aggregation.

RECOMMENDATION 5:
Agreed standards for Obfuscation/Perturbation

As a complementary Recommendation to 4, standards should be agreed for obfuscation and perturbation. This can not only help provide confidence that data has been robustly de-identified, it can also help with the creation of minimum cohort sizes.

RECOMMENDATION 6:
Develop and promote open data enablers

In support of Recommendation 2, develop in-depth guidelines on anonymisation and de-identification that, like those issued by the UK Office of the Information Commissioner, consider a balanced approach to the risk of harm resulting from any reidentification .

RECOMMENDATION 7:
Establishment and maintenance of a dataset of issues arising from Privacy Impact Assessments

Much of the data being shared has been collected with some form of express or implied consent, for some specific purpose. Respecting this consent while supporting sharing will be a major challenge in establishing effective 'privacy preserving' frameworks. As Australia's experience with health data has shown, communication and consent contributes to trust and support for sharing. As the experience in the UK has shown, adoption of systems that facilitate an anticipatory regulatory approach ensure risk identification, classification, and appropriate mitigation/remediation strategies are identified and developed.

40.Available online http://www.ipc.nsw.gov.au/sites/default/files/file_manager/Conditions_Enabling_Open_Data_Report_Final.pdf (Accessed 6 August 2017)

Glossary

DATA SET
An individual database, collection of databases, or a defined set of data across one or more databases.

DIFFERENTIAL PRIVACY
A method for introducing mathematical noise to data sets to obscure the source data while maintaining the ability to draw conclusions from the data in an aggregate manner. Differential privacy aids in the prevention of de-anonymisaiton between one or more anonymised databases where, if linked, personal information could otherwise be inferred.

FIVE SAFES FRAMEWORK
A framework designed to assist the decision making process as it applies to confidential or sensitive data, categorising use of and access to data into the five dimensions of projects, people, settings, data and outputs. Initially designed by the UK Office for National Statistics (ONS), it has since seen widespread use outside of the UK including the Australian Bureau of Statistics (ABS).

HOMOMORPHIC ENCRYPTION
A method of performing calculations on encrypted data, producing an encrypted result, which when decrypted matches the result of performing the same operation on original unencrypted data. As a result homomorphic encryption can be used to perform calculations on data while masking the content of that data.

K-ANONYMITY
A model by which data is supressed (e.g. fields replaced with '*') or generalised (specific attributes replaced with generalised attributes, e.g. Age 21 → [20-30]) in order to obfuscate personally identifiable data while retaining the ability to return sufficiently accurate results operating on the data set.

L-DIVERSITY
An extension of K-Anonymity to further prevent individual identification, or attributes belonging to an individual, that could be inferred by the data - e.g. where a given attribute for a set of records is the same, and thus that attribute becomes a known value rather than an obfuscated one. L-diversity improves on this by ensuring common values appear less frequently and uncommon values appear more frequently.

PERSONAL INFORMATION FACTOR

A value defined as a quantifiable volume of information for the purposes of identification. In this white paper, the factor is defined from 0 (anonymity) to 1 (identified individual).

PERSONALLY IDENTIFIABLE INFORMATION

Any information or data that, in whole or in part, can be used to identify, locate, or contact a single individual. Typically, PII is used as a benchmark with respect to security and privacy for the purposes of risk management. Also known as Personally Identifiable Data (PID) or Sensitive Personal Information (SPI).

PRIVACY PRESERVING LINKAGE

A technique by which links between records in databases are maintained in such a way as to not compromise individual privacy. This requires identifying which record linkages between two or more databases that correspond to an individual, and implementing techniques to obfuscate the source data while maintaining the ability to run queries on linked data.

Thanks

The Data Sharing Taskforce has been run as a series of workshops and occasional intermediate conversations. Workshop participants provide their time freely to help address the challenges within the scope of the Taskforce. Participants are free to join or not join each workshop. Special thanks go to some of the more diligent, enthusiastic contributors of these workshops:

Stephen Hardy, Peter Leonard, Geof Haydon, Frank Zeichner, Scott Nelson, Geoff Clarke, Ashton Mills, David Marcus, Sonya Sherman, Ghazi Ahamat, Jeremy Moon, Passiona Cottee, Shveta Gupta, Chris Radbone, Varant Meguerditchian, Ben Hogan, Evan Holley, Jeremy Harris, Nick von Sanden, Rolf Green, Justin Poole, Malcolm Crompton.

Thanks also to all others who have made, and continue to make, contributions and feedback.

Finally, the ACS Policy Reference Group would like to thank the Data Sharing Taskforce for their important work in exploring and building these first steps to data sharing frameworks, and for the production of this white paper.

ABOUT THE ACS

The Australian Computer Society is the professional association for Australia's Information and Communications Technology sector.

We are passionate about recognising and developing ICT skills and provide more than 60 products and services to our members. We are also the voice of Australian ICT, representing all practitioners in business, government and education.

In everything we do, our goal is to advance ICT in Australia and help our members be the best they can be.

ACS
Level 11
50 Carrington Street
Sydney NSW 2000

P: 02 9299 3666
F: 02 9299 3997
E: info@acs.org.au
W: www.acs.org.au