TELSTRA CORPORATION LIMITED

Submission to the Productivity Commission’s Inquiry *Data Availability and Use*

29 July 2016

CONTENTS

Executive summary

In recent times the level of data within the economy has increased significantly, reflecting the growth of digitisation in many areas of economic activity. While digitisation has already created a range of benefits for consumers and businesses there is interest in further harnessing this change to further improve the living standards of all Australians and help promote ongoing economic growth. As Australia's leading telecommunications and information services company, Telstra understands and shares this objective.

Telstra, in managing data, is committed to respecting the interests of its customers at all times. We use data to support the ongoing provision of services to our customers, are fully compliant with our privacy obligations and invest significant resources in protecting the data which we hold. Our customers trust us to be the custodians of their data, and we take this responsibility very seriously.

While the inquiry area is broad we have identified two key inter-related considerations for improving the use and availability of data in Australia as outlined below.

The nature of data underpins use and influences availability

Telstra believes that the nature of any given data (or dataset) not only underpins its use but can also influence its availability. This proposition is generally apparent with reference to public sector datasets and private sector datasets — where they exist, the former tend to be available whereas with the latter, commercial interests can come into play and limit availability. The data we hold is predominantly customer or network related in nature, and accordingly is used by us in a business context. Because this data underpins our operations, we see it as being proprietary in nature and generally do not make it publically available. We note that public interest considerations also weigh against the disclosure of information on telecommunication networks, especially locational data, as this could lead to infrastructure being targeted by criminal and/or terrorist activity.

We do, however, consider providing access to our datasets where we can see the benefits of making data available and enter into release arrangements consistent with our privacy obligations and information security controls. We also share certain network-related data voluntarily in some circumstances. We are not supportive of any moves to mandate the sharing of private sector datasets through regulatory measures because this would have an adverse effect on our business, impacting both our customer relationships and investment decisions.

Policy settings are still evolving, consumers are still adapting

One consequence of the rapid growth in both data and digitisation is that policy settings are still evolving to reflect these changes and similarly, consumers are still adapting. In order for the benefits of increased data use and availability to be fully realised it is essential that policy settings in data-related areas are fit for purpose and consumers have confidence and trust in how their data is collected, stored and used.

In the context of privacy Telstra has recently had to consider the question of whether telecommunications metadata — that is, information about a communication that is not the content of the communication — is 'personal information'. This experience has created uncertainty about what data is subject to privacy law.

In relation to consumer adaptation, information asymmetries and behavioural considerations may be limiting the confidence and trust people have in the use and sharing of data (including their own). This is understandable as many people would have little familiarity with advanced analytical techniques such as data de-identification and machine learning algorithms, and people are often reluctant to embrace change. In light of the benefits — including benefits for consumers — that are associated with increased data use and availability, there may be a role for government (in conjunction with industry) to develop education and awareness campaigns in these areas and actively support the process of adaptation.

01 Introduction

Telstra welcomes the opportunity to respond to the Commission's recent Issues paper on 'Data Availability and Use'.

We note that the Commission has been asked to investigate the benefits and costs of increasing the availability and use of public and private data in Australia, and provide recommendations on how data access can be increased while enhancing confidence in the way data is collected, stored and used bearing in mind privacy and data security considerations.[1] This is a broad remit, encompassing issues that have had varying levels of exploration and policy response by government in recent years.

As Australia's leading telecommunications and information services company, Telstra has a strong interest in issues pertaining to the use and availability of data. In addition to being the direct provider of many data-orientated services to consumers, businesses and government, our telecommunications network is a substantial enabler of these services more broadly.

Data can take various forms, most frequently words and numbers, and can be created from almost any activity within the economy today. As noted by the Commission, data can have little if any meaning without being put into context, but once this occurs through processing of some form, information may be derivable.

It is the coincidence of increasing digitisation, leading to increased data generation, and enhanced computing power and analytical capabilities which has led to the creation of new business models and attracted interest in the broader economic potential of data through use. Each of these propositions is exciting, and Telstra believes there is considerable scope for data and its use to contribute positively to economic growth, productivity and consumer welfare in the years ahead.

Realisation of these benefits, however, will be contingent on policy settings which encourage private sector investment and innovation in relation to data and its use, and promote consumer confidence and trust in the collection, use and sharing of data.

This submission begins with a discussion of issues that we see as being central to 'data use and availability', reflecting our perspective as a key private sector entity. Following this, we consider some of evolutionary and adaptation challenges which exist for policy frameworks and consumers respectively due to the increased level of digitisation within the economy and associated increase in data.

[1] We also note that the current inquiry follows a recent Commission research paper (*Digital Disruption: What do governments need to do?*) and the Harper Review of Competition policy, and a related inquiry is also underway (*Intellectual Property Arrangements)*.

02 The nature of data underpins use and influences availability

The inquiry area 'Data use and availability' is broad and encompasses numerous policy considerations. As a large company which holds a reasonable amount of data, Telstra believes that the nature of any given data (or dataset) not only underpins its use but can also influence its availability. Further, while there may be many use cases for any given data, the existence of this data does not necessarily result in its availability for use by others.

In this section we highlight the differentiated nature of public and private sector datasets, and the general effect of this on their respective availability. This is followed by greater detail on the nature of the data held by Telstra, and several examples are provided to show how we use our data in different business contexts. This section concludes with the consideration of availability and access questions, with particular focus on private sector datasets as this is where our experiences have been concentrated.

2.1. Public and private sector datasets differ from each other

While the Issues paper encompasses both public and private sector datasets, these are quite different in their nature and correspondingly, questions of use and availability have varying applicability.

Public sector datasets cover a wide range of areas and topics, and their number is set to grow in coming years due to efforts to improve availability. This data, where available, is used by both private and public sector bodies, with the most requested forms of data presently spatial and land, socio-economic, health and transport. Within the public sector restrictions on availability do exist, with personally identifiable data classified as being the most sensitive type of data. This sensitivity increases as this data is linked (for example, linked tax and social security data). Significantly, motivators for increasing the availability of public sector data include enabling innovation outside the Australian Public Service and enabling smarter, citizen-centric services and policies to be developed.[2]

In contrast private sector datasets tend to reflect the business operations of the relevant data holder or compiler, and while the number of these is increasing due to digitisation and innovation, actual availability is a separate issue with access typically dependent on some form of commercial negotiation. In some cases 'compilers' may provide their datasets to third parties under contractual arrangements to support service provision of one form or another.

2.2. Telstra's data is largely proprietary

The data which we hold primarily relates to our customers, the services we provide to them and our network infrastructure. We do note, however, that our data has an inherent breadth and it is difficult to capture all of its attributes in a limited discussion such as this.

Following from the above, and for the purposes of this submission, our 'private sector datasets' can be characterised as being either customer datasets or network datasets. In practice there is some crossover between these, because service provision to customers typically utilises our networks.[3] Separate to these datasets, we also hold data as a third party (under commercial arrangements) in the context of services provided by Telstra Health. Maintaining customer privacy is taken very seriously when analysing any type of dataset.

We see our customer and network datasets — used for activities such as market segmentation, product development and refinement, forecasting for future growth, network operations, customer service and

[2] Page 11 of this recent project by Department of Prime Minister and Cabinet identified areas of potential innovation: https://www.dpmc.gov.au/sites/default/files/publications/public_sector_data_mgt_project.pdf

[3] It is also the case that that within our customer datasets there is an important distinction between Wholesale and Retail customers, which we are required to ring-fence for regulated services as part of our structural separation obligations.

billing — as being central to our business and largely proprietary in nature.[4] For these reasons we invest significantly in the physical and cyber security of our systems, limit access as appropriate, actively monitor our networks and systems, invest in an effective security monitoring and response capability and provide training for our staff on the importance of protecting customer data and our associated legal and regulatory obligations.

As a precursor to the use examples and following discussion we feel it is important to emphasise that:

a) At all times Telstra is committed to protecting our customers' privacy, keeping their personal information safe and ensuring the security of their data;

b) We comply with the *Privacy Act 1988*, Australian Privacy Principles and other regulatory measures to give customers appropriate 'opt in' and 'opt out' control with respect to direct marketing; and

c) We would only disclose identified customer data to third parties after collecting the appropriate consent. For disclosures of de-identified data we have sought to develop and implement leading privacy protection techniques to mitigate the risk of that data being re-identified.

2.3. Use in a business context

Because our customer and network datasets, by their nature, relate to our business activities they are accordingly used in a business context.

In an applied sense the 'business context' can vary — it may, for example, be services which we provide direct to customers in a retail or wholesale capacity, the network infrastructure used to provide services or other services we provide to (or in partnership with) third parties — but the common denominator is provision by Telstra, using Telstra's customer data and/or network data.

The slight nuances around 'business context' are illustrated via the three use examples below.

1. *Retail services as the business context*

   Mobile services in Australia are currently provided using second, third and fourth generation mobile technologies — colloquially these are known as 2G, 3G and 4G. On 1 December 2016 Telstra will be discontinuing its 2G network, meaning devices that only operate on this network will stop communicating with a network at this point in time.[5] Because it is an older technology, 2G devices tend to be relatively simple and are either a basic mobile service (voice and limited data) or a machine-to-machine (M2M) service. From a business perspective the discontinuation creates challenges of alerting the relevant account owners that their device will soon stop working, and then identifying an appropriate migration option for these customers. To address these challenges Telstra has used network data to identify all devices that are registering on our 2G network and identify the type of activity they are engaged in (i.e. is the device part of M2M communication?). This information in turn allows account owners to be contacted (noting you cannot constructively contact a machine) and recommendations made about what service will best suit their needs moving forward.

2. *Network infrastructure as the business context*

   Our network is central to ongoing provision of services to customers. In order to improve the reliability of our services we have recently combined data on current customer fault reports with historic network element failure patterns and network topology data to pre-emptively identify network elements where routine maintenance work could be brought forward to help prevent faults occurring. We see this use of data as being beneficial for our customers, noting the data used is

[4] It is noted that some data which is not central to our daily business operations is held in compliance with regulatory obligations we face. One example of this is the Data Retention legislation to which we are subject.

[5] The reason these devices will stop working is because the frequency bands (i.e. spectrum) they use will be repurposed for another use, and as such the registration of 2G devices on these will not be permitted. 3G and 4G devices operate on different frequency bands.

itself on distinct characteristics of our various networks (i.e. the incidence of a given fault *and* the age and location of similar or identical equipment). Because the context is network maintenance, data on current faults is given commercial meaning through its combination with other network information.

3. *Services to third parties as the business context*

In a public policy setting, Telstra is a participant in the government's emergency alert initiative (EAI).[6] The EAI uses several data sources to provide voice and text alerts to people in locations where there is a bushfire threat or some other natural disaster event. These include:

- The integrated public number database (IPND), which is an industry-wide database containing all listed and unlisted public telephone numbers; and
- The location based number store (LBNS), which holds telephone number and the associated address data drawn from the IPND, and also assigns a latitude and longitude value to each fixed line number, using information from the Geo-coded National Address File.

When an emergency event occurs, emergency service organisations contact network providers such as Telstra to issue emergency alerts to people in affected areas using the IPND and LBNS. Geocoded information allows alerts to be transmitted via the relevant fixed line numbers while a technology known as 'location based solutions' allows alerts to be transmitted to mobile phone services which are in affected areas. These alerts to mobile services combine data from the IPND with real time network data held by the operators of mobile phone networks. Because mobile phones are continually registering with their closest mobile phone tower to enable connectivity, network operators can tailor the delivery of alerts to those mobile services which are within range of a given mobile phone tower. This aspect of the EAI uses network data from Telstra (and the other operators of mobile networks), with the context — i.e. recognition that a given mobile service is in an emergency area — giving it meaning.

The EAI is a public policy undertaking based on disaster management and public safety rationales, with the initial funding provided by the Commonwealth Government and ongoing costs met by each state and territory government. In this example, the characteristics of the data which are of value are the locational information, encompassing both fixed line services and mobile services on a real time basis.

One aspect of the EAI example which is particularly notable is the way in which the privacy of customer information is maintained at all times. No emergency service organisation has direct access to telephone numbers when warnings are sent through the emergency alert system and information on telephone locations is not retained by the network operators effecting the warnings. This is significant because the 'value' (i.e. awareness of an impending threat) is created for customers via the use of their customer data in conjunction with network data, but their details are not actually revealed to anyone. This approach mitigates various risks related to potential abuse of the service by hackers in order to reveal personal location information.

Because our customer and network datasets are central to our business (as illustrated), this influences the extent to which we are willing to make them available to other parties.

2.4. Availability and access

Within the Issues paper there are a range of questions about the availability of public sector datasets and the accessibility of private sector datasets. Because we are more familiar with private sector datasets than public sector datasets, our views in this area are presented first.

[6] See http://www.emergencyalert.gov.au/

Private sector datasets

The Issues paper correctly recognises that private sector datasets are not generally available, and because they can contain information relevant to competitive activities they must be 'accessed' (as in, access is provided by the relevant data holder or compiler). Telstra agrees with this proposition because it clearly implies that private datasets have value and some type of commercial arrangement will typically be required before any data is made available.

The trust customers place in us as custodians of their data is the primary reason why we do not disclose our customer datasets. Legislation which prohibits the unilateral disclosure of certain customer data and the inclusion of confidentiality clauses around some of the services we provide are also reasons why we do not make our datasets publically available, noting they underpin our operations, are a source of commercial value and involve cost in terms of collection and management activities.[7]

Telstra and other telecommunications service providers are subject to obligations which restrict the use and disclosure of certain types of data, for example obligations under Part 13 of the *Telecommunications Act 1997*.[8] In conjunction with these and other competition related obligations, we would typically view questions of access to private sector datasets — including any access to Telstra's datasets — as being in the domain of commercial negotiations, reflecting their proprietary nature.

Telstra is a limited participant in voluntary data sharing arrangements. One example of voluntary data sharing is our involvement in the 'Dial before you dig' initiative.[9] Under this initiative information on the location of underground utilities is provided to excavators and other tradespeople, protecting them from workplace risks and simultaneously protecting our infrastructure (and that of other utility providers) from unintended disturbance. Where proposals for voluntary data sharing arrangements arise we would consider these from a whole-of-business perspective, and be mindful of any possible competition issues which could result.

In terms of standardisation, we note that in emergent areas such as the internet of things (IoT) and '5G' technology there are various industry initiatives aimed at promoting the development and use of common data standards. Attaining some level of standardisation is important across a range of IoT sectors such as health, education, electricity and transport as this in turn will enable the development of multi-purpose devices and collaborative applications. In some instances there is a multi-lateral dimension to these standardisation efforts, and this is the case with 5G technologies which are expected to underpin numerous IoT applications as well as future mobile phone cased communications.

There are two public interest considerations which weigh against the disclosure of information on telecommunication networks, especially locational data. Firstly, telecommunication networks play an important role in supporting public safety by enabling public agencies to respond to emergency situations when they arise. Secondly, because telecommunication networks are essential infrastructure they would be a target for criminal and/or terrorist activity if information about their location was publicly available.

Consistent with the positions above, Telstra does consider providing access to one or more of our datasets where we can see the benefits of availing data and come to release arrangements that are consistent with our privacy obligations and information security controls. That said we are continually exploring ways to use our data in new and constructive ways for the mutual benefit of our customers and our business and because of this, and the nature of our datasets, we would not be supportive of moves to mandate the sharing of private sector datasets. Such a development would have an adverse effect on our business, impacting both our customer relationships and investment decisions.

[7] We do, however, willingly comply with Australian Privacy Principle number 12 — providing individuals with access to the personal information we hold about them upon authenticated request — but this scenario is clearly distinct to availing a dataset in entirety.

[8] See the ACMA Fact sheet: http://acma.gov.au/~/media/National%20and%20community%20interests/Fact%20sheet/pdf/Disclosure%20requirements%20under%20Part%2013%20of%20the%20Telecommunications%20Act.pdf

[9] See: https://www.1100.com.au/

Public sector datasets

Telstra makes use of a subset of the available public sector datasets, such as the Geocoded National Address File (G-NAF) and is supportive of moves to increase their availability. Conceivably there may be opportunities to combine public sector datasets with telecommunications network data we hold — such as areas of mobile phone coverage — and we are exploring these opportunities in greater depth.

Telstra is also supportive of moves to explore possible standardisation frameworks for public sector datasets, noting some initial work in this area has been undertaken by the Department of Prime Minister and Cabinet. While such frameworks may not be immediately applicable to private sector dataset given the underlying differences in the nature, some learnings — especially on matters of sensitivity, and the management of these — may be possible.

In general terms we believe that greater availability of public service datasets can help provide greater accountability in the delivery of public services, support performance monitoring and inform consumer choice. For example, in social service areas such as health, greater availability of data on public hospitals could inform performance benchmarking between different public hospitals, and support accountability of those services to the public. For these reasons we support the ongoing investments by Governments across Australia in improving the quality and breadth of their datasets, and exploration of ways to make these open and available for use by third parties.

03 Policy settings are still evolving, consumers are still adapting

The area of 'Data use and availability' has undergone considerable change in recent years, growing in scale, scope and complexity. This change, which is likely to continue into the future, requires the ongoing evolution of policy settings so they are fit for purpose and inevitably requires a degree of consumer adaptation as well.

In this section we discuss one specific data-related policy setting which may not be fully fit for purpose, namely the legislative definition of 'personal information'. Attention is also focussed on several data related areas where adaptation challenges for consumers, including behavioural considerations, may exist. These include having confidence and trust in data holders, an understanding of and comfort with advanced analytical techniques and having an awareness of cyber-security and the protective measures implemented by organisations such as Telstra.

3.1. With privacy frameworks, uncertainty and potential policy conflicts exist

Australia's privacy framework has undergone various reforms in recent years. The framework is now centred upon the Australian Privacy Principles (APPs), which took effect in March 2014 and replaced the previous National Privacy Principles (NPPs). Telstra, as a strong supporter of privacy, participated in the consultation process associated with the introduction of the APPs. The central concept within each set of principles is 'personal information', for which specific management and handling provisos apply.

In August 2013 a complaint was made against Telstra to the Office of the Australian Information Commissioner (OAIC) which claimed we had breached the complainant's privacy by refusing to provide access to metadata information relating to the complainant's mobile phone service.[10] While the OAIC made a finding against Telstra, this was successfully appealed in the Administrative Appeals Tribunal (AAT).[11] The OAIC has now appealed the decision to the Federal Court of Australia.[12]

The term 'metadata', as it is used in relation to telecommunications, is generally understood to mean information about a communication that is not the content of the communication. This may include the types of information that appear on a billing record, such as the time, date and duration of a telephone call. Metadata may also include what is described as 'network data. For example, the recorded transactions that occur between a device and a telecommunications network which occur to manage the mobility of the device through the network, and also occur to establish, maintain or disconnect connections between the device and destinations it is seeking to communicate with. While we accept that 'personal information' in the NPPs (and/or subsequent APPs) may cover information such as a billing record, we do not think that it covers network data.[13] This question is now the subject of the appeal to the Federal Court and as such the definition of personal information is currently uncertain for us and any other organisations which generates metadata that is not linked to the identity of the customer. More broadly the current situation exemplifies the challenges that rapid technological changes — including the creation and storage of ever increasing amounts of data — create for privacy frameworks in Australia.

[10] Australian Information Commissioner. AICmr35. 1 May 2015. http://www.austlii.edu.au/au/cases/cth/AICmr/2015/35.html.

[11] Administrative Appeals Tribunal of Australia. AATA-991. 18 December 2015. http://www.austlii.edu.au/au/cases/cth/AATA/2015/991.html

[12] AIC Media Release. https://www.oaic.gov.au/media-and-speeches/statements/privacy-commissioner-lodges-appeal-to-federal-court-re-telstra-corporation-limited-v-privacy-commissioner 11 February 2016.

[13] While the initial finding was made under the NPPs, there would appear to be potential for a similar finding under the APP's (which apply today) but this has not been formally tested by the courts.

In the context of data use and availability, our primary concern is that should the original decision of the Privacy Commissioner ultimately stand this will require Telstra to re-architect its internal systems in order to link network metadata to individuals in a manner which would allow us to manage any future metadata requests. Such an undertaking would involve us incurring compliance costs that would appear to be considerably greater than any individual 'access' benefit (breaching a fundamental principle of regulation) and would also result in the creation of a centralised data repository for customer network data. This repository could be an attractive target for hackers and criminals (despite the fact we would deploy advanced protective measures), creating a new frontier of risk for the privacy of all customers. Instead of protecting personal information, Australia's privacy regulations could expose such data to greater risk. Such an outcome would reflect a conflict between policy and regulatory objectives, and would be likely to have a negative impact on data use and availability.

Depending on the outcome of this matter, the Commonwealth may need to revisit the APPs to ensure that the definition of personal information is appropriately fit for purpose and devoid of any uncertainty, especially that attributable to technological change.

3.2. Supporting consumer adaptation

Increasing digitisation within the economy and the associated increase in data represents a substantial change in the conduct of daily activity for many people, and potentially gives rise to adaptation challenges for some consumers. Anecdotally, some of these challenges appear to have a behavioural element but equally they may be broader in nature — as in some type of structural adjustment — noting the Commission has identified digital disruption as a source of structural change in the economy.[14] It is also possible that some consumers are unfamiliar with the advanced analytical techniques which have emerged in data-related areas.

Specific areas where adaptation challenges could exist include building confidence and trust in data holders, being comfortable with advanced analytical techniques and having an understanding of cyber security and the risks which exist in this area. In the interests of realising benefits from digitisation and mitigating risks, these are all areas where some role for a government education program may exist, potentially in conjunction with industry.

Building confidence and trust

As noted in the Issues paper, in order for the economic benefits of data to be fully realised it is essential that consumers have confidence and trust in how data is collected, stored and used. Telstra agrees, noting we have a strong commercial interest in ensuring our customers continue to trust us to appropriately manage, use and protect their data at all times.

While Australia's privacy principles play an important role in creating confidence and trust by giving consumers an element of control over how their data is used, this confidence and trust can be fragile and weaken quickly. This fragility may be attributable to a combination of information asymmetries and/or behavioural considerations.

For various reasons there may be information asymmetries between consumers and data holders about different aspects of how data is collected, stored and used. For example, consumers may not be familiar with machine learning algorithms, their purpose and/or the fact they often use data which has been de-identified. To some extent information asymmetries can be addressed by targeted education and information provision, and both government and industry may have a role in promoting more clearly the benefits of increasing data use and availability and addressing concerns which exist in these areas.

Behavioural considerations exist in all spheres of the economy, and are likely to have some applicability to the area of data use and availability. Researchers have established that subconscious cues can

[14] http://www.pc.gov.au/research/completed/digital-disruption/digital-disruption-research-paper.pdf

trigger behavioural responses, and these can be challenging to respond to in practice.[15] Two well-known behavioural responses which could influence consumer trust and confidence in data-related areas include the availability heuristic and cognitive dissonance.

With the availability heuristic, people tend to rely on available information, so where for example there is a data breach reported in the media they could think this is likely to happen them. In this scenario the probability of a negative event may be overestimated, and there is no consideration of factors like the security controls their service providers may have and how these might differ from the firm which suffered the initial breach.

With cognitive dissonance, people can periodically exhibit inconsistent thoughts or attitudes. In the context of data-related areas, many people strongly value their privacy but can also act in an inconsistent manner by forgoing aspects of their privacy in order to get some type of benefit.

Managing potential behavioural considerations is an issue for building consumer confidence and trust in how data is collected, transmitted, stored and used. There may be a role for government in targeting specific behavioural factors through education and awareness campaigns in the interests of increased data use and availability in Australia. Industry may also be able to assist with this task.

Advanced analytical techniques & understanding use

Digitisation and its associated increase in data volumes have also been accompanied by advancements in analytical techniques for large data sets. These techniques are often grouped under the term ‘big data analytics’ and are typically geared towards finding patterns, correlations or other insights within a given data set. Big data analytics can enable these types of outcomes to be realised more quickly than other, less sophisticated approaches. Telstra is among the companies investing resources in the area of big data.

Given they are a reasonably new development and encompass significant computing power, the nature and purpose of ‘big data’ analytical techniques may not be well understood by consumers. Specifically, consumers may not be aware that ‘big data analytics’ are often undertaken on datasets which have been de-identified, meaning privacy considerations are fully adhered to. Because the focus is on identifying insights from aggregated data or information, raw individual-level data is not revealed within analytical activities (noting de-identification may also have occurred).

In practice de-identification entails, at the very least, removing key identification attributes such as name, address, phone numbers and membership numbers. Whilst this may suffice to de-identify the data for many use cases and contexts, there can be re-identification risks which may need to be mitigated with additional processing and control. For example, it may be possible to re-identify some datasets by linking those with other datasets that are not de-identified.[16] Because of this risk additional layers of protection can be applied, with these techniques including k-anonymisation (grouping data together so that insights reflect groups of at least ‘k’ people) and differential privacy (adding ‘noise’ to the data so that an attacker cannot use the differences between one dataset and another to infer something about an individual).

Another technique for using customer data without breaching privacy considerations is machine learning, or machine learning algorithms. In these use cases, customer data is an ‘asset’ from which a machine learning algorithm can ‘learn’ a pattern. This algorithm can then be exposed outside of the organisation, and reflect the education from the ‘lessons’ (i.e. the insights) without necessarily exposing what was ‘taught’ (the data).

Telstra’s main investments in big data involve enabling better maintenance of our networks, which — as the largest in Australia — covers thousands of kilometres, entails around 5000 exchanges and has

[15] The UK’s Institute for Government has published a useful report on the implications of behavioural theory for policy making which considers this issue. Refer to: http://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf

[16] Refer to Narayanan and Shmatikov (2008) for a case study on this issue: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

extensive on-the-ground assets in the form of ducts, mobile towers and underground fibre. As big data applications mature the potential for them to deliver benefits to consumers is likely to increase. In order to enable both current and future applications of big data, and the benefits which they can deliver, it will be important that they are accepted by consumers. To this end, some education about big data, its interface with privacy frameworks and the benefits it can deliver may be required.

Cyber security

Cyber security involves the adoption of protective measures for data and information held electronically by individuals, companies and governments. While the growth of digitisation has delivered benefits for these groups, it has also been accompanied by increasing cyber risk and the incidence cyber-crime. For these reasons cyber-security is of significant importance, especially for data holders such as Telstra.

Cyber security is a complex area and a matter Telstra takes seriously, with an entire team dedicated to protecting the data we hold and our network. As a network operator Telstra is involved in cyber security activities at both the wholesale and retail levels of our operations, both internationally and domestically. In practice cyber security can effect data security (as well as broader security, such as network security), meaning these particular systems need to be implemented in a way which is consistent with the *Privacy Act 1988* (including the protection of personal information). We believe that our security controls represent industry best practice, are and in alignment with our customer expectations and contractual obligations.

While cyber security is commonly perceived as a technical undertaking, maintaining security is not solely dependent on technical solutions. Anecdotally, for many cyber incidents which result in data breaches there is a human element at fault such as an individual opening a phishing email and clicking a malicious link. This is not a failure of any technical element, and underscores the importance of having training and awareness programs for staff who access or maintain data, or use systems in which data is kept. Such programs must be provided in addition to having technical checks and balances (i.e. automated controls) in place and well-documented, well-maintained operational processes. Less obviously — and linked to the discussion in the preceding section — data breaches caused by human error can have a detrimental impact on consumer trust and confidence in cyber security frameworks because it is the systems, not the people operating them, that are perceived to be at fault.

Telstra is supportive of mandatory data breach reporting being introduced in Australia, and sees this measure as important in helping to build consumer confidence and trust in the holders of their data. We note that pending passage of the data breach legislation, we have adopted reporting protocols which are consistent with the "*Data Breach Notification – A guide to handling personal information security breaches*" paper published by the OAIC.[17]

[17] https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches