IT'S HOW WE CONNECT

Telstra's submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

1. Introduction

Telstra appreciates the opportunity to provide this submission to the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) inquiry on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (**Data Retention Bill**). In addition to this submission, we have contributed to the joint submission already made to the PJCIS by the industry associations Communications Alliance and the Australian Mobile Telecommunications Association. We have also participated in the Government's Data Retention Implementation Working Group and contributed to its report.

Lawful access to telecommunications data is an important tool for Australian law enforcement and national security agencies (**agencies**) that helps save lives and solve serious crimes in this country. Given the changing security threat environment both domestically and internationally, and the fact the telecommunications sector is experiencing rapid technological transformation, we understand the reasons behind the decision to introduce legislation mandating a data retention scheme.

Nonetheless, a data retention scheme is seen as intrusive by some of our customers. It will also impose significant complexity and costs on the telecommunications industry, while having data security and privacy implications. These issues are discussed in more detail later in this submission.

In making this submission we are seeking to contribute to striking an appropriate balance between delivering the public good of community safety on the one hand and meeting Australian consumers' expectations of privacy while minimising the regulatory burden imposed on industry on the other. In our view, the best way to achieve this balance is to ensure any data retention scheme:

- Is proportionate to the threat level;
- Applies equally to all industry participants who supply services to customers in Australia;
- Is practical, cost-effective and provides long-term certainty for industry and our customers about what data telecommunications companies are required to retain;
- Places appropriate limits on who can access the data and under what circumstances they can do so; and
- Puts appropriate oversight mechanisms in place.

2. Customer expectations

Telstra is Australia's leading telecommunications and information services company, offering a full range of communications services and competing in all telecommunications markets. We currently provide more than 32 million voice, internet and email services in Australia across our mobile and fixed networks and BigPond email platform. Our customers are at the centre of everything we do at Telstra. The goal of meeting their expectations of privacy, while providing lawful assistance to the agencies to protect the community, underpins our approach to the issue of data retention.

Our current commercial data management practices are limited to collecting and storing certain information that is relevant to providing our services, managing our networks, and developing new products and services. For example, the data we currently collect and store about our customers includes names and addresses, call records and the amount of data consumed so that we can provide our services and bill accurately for them.

The data we collect for commercial purposes can already be lawfully accessed by agencies in line with the obligations imposed under the Telecommunications Act (Cth) 1997 and the Telecommunications (Interception and Access) Act (Cth) 1979. Recently, we published our first annual Transparency Report detailing the lawful requests for assistance we received from the

agencies in the financial year 2013-14. The report detailed that we acted on around 85,000 direct requests from law enforcement agencies for customer data last year, of which 2,700 were warrants for access to content.[1]

In our experience, any increase in the amount of data we are required to collect, store and make available to agencies about our customers will be a cause of concern for at least some of our customers. This is particularly the case where the additional data does not serve a commercial or technical purpose related to their service, and/or if the data is web browsing history, email content and mobile phone location (all of which are linked to heightened public sensitivity).

In developing the Data Retention Bill, the Government has demonstrated they are aware of many of these concerns. We understand this has informed the Government's decision to limit the scheme to metadata and not the content of communications, and to limit the agencies that can access the data to those involved in criminal and national security investigations. We welcome such limits, as we believe they will help give the community a greater degree of comfort about the use of telecommunications data by the agencies.

3. **Regulatory burden and costs**

If enacted, the legislation will require Telstra to collect and store certain types of data for two years and to make this data available upon request to law enforcement and national security agencies. Based on the data set proposed by the Government, this requirement goes beyond Telstra's current commercial practices and will impose a new regulatory burden and create costs for our business.

For example, the draft data set includes, among other things, originating IP addresses for internet browsing sessions from mobile devices, call records on attempted calls that are not connected and the size of emails. These are forms of data that we do not currently retain in an accessible way as part of providing services to our customers.

Telstra shares the general view of industry that as the cost of this new activity is unrelated to providing services to customers or managing our networks, but is being imposed by Government, public funding should be available to compensate for the upfront capital costs associated with the Data Retention Bill. Further, the principle that we neither profit from, nor bear the costs of, providing reasonable assistance to agencies should apply to the ongoing operating costs incurred in providing access to this data.

Based on information available to date, we forecast the upfront capital cost associated with building the system necessary to comply with the Bill to be significant. The capital costs will be incurred in building a centralised mediation platform to extract, store, retrieve and process the required telecommunications data for the agencies. In addition, we will need new systems and interfaces between this platform and our existing network elements to extract data we do not currently collect today. Such a platform would be similar to the systems deployed by telecommunications companies in European countries (such as the United Kingdom) that have at one time mandated data retention obligations in recent years.

Telstra's forecast capital cost does not include the ongoing operating costs of complying with agency requests for data and other potential costs that are detailed later in this submission. We have provided a more detailed account of Telstra's forecast capital costs to PriceWaterhouseCoopers (PWC) as input to the cost assessment work they are undertaking on behalf of the Government. The information provided to PWC is commercial-in-confidence.

[1] This excludes requests related to national security. The Telstra Transparency Report is available here: https://www.telstra.com.au/privacy/transparency.

IT'S HOW WE CONNECT

4. **Certainty on the obligations**

It is the amount of new data that we have to collect, secure, index, store and retrieve, combined with the number and complexity of systems that data transits through today, that will determine the ongoing cost impact of this scheme on Telstra.

We recommend that in order to limit the impact and costs associated with the proposed scheme the obligations imposed on industry are as simple, clear and as close to existing commercial practices as possible. Telstra recognises there are differing positions on the length of time for which data should be retained under the scheme. From our perspective, given the number and complexities of the systems we operate, Telstra would prefer a single fixed data retention period across all technologies and data types.

To further minimise the compliance burden and cost, there should be long term certainty on the data set. Changes to the data set – either by introducing new types of data to be retained or altering the existing requirements – has the potential to impose significant new costs to industry. This extends to changes to the form that Telstra is required to retain the data and make it available to agencies and the retention period.

As we and other industry participants will be designing and building new systems in order to comply with the data retention obligations, now is the time to set and fix as much of the detail of these obligations as possible. Any uncertainty or changes to the obligations – even seemingly minor ones – has the potential to create significant complexity and cost for industry. To this end, we believe any changes to the scope of the regime, including changes to the data set and retention period, should only occur after consultation with industry, be subject to Parliamentary oversight and allow sufficient time for companies to comply with the change or apply for an exemption.

5. **Level playing field**

To promote clarity and to ensure that the new obligations do not put certain technologies or companies at a commercial disadvantage, it is important any new obligations apply broadly and equally.

This means that the obligations should be technologically agnostic to the greatest extent possible. For example, one set of retention obligations should not apply to traditional technologies, such as PSTN or mobile voice and SMS services, while different obligations apply to competing technologies, such as Voice over IP or instant messaging. Not only would asymmetric regulatory obligations put providers of the traditional services at a commercial disadvantage, it would create a perverse incentive for criminals to circumvent scrutiny by the agencies by using the alternative services. To avoid these problems, the new data retention obligations should create a level playing field and apply equally to any company offering communications services to Australian consumers.

Similarly, if the obligations are only imposed on companies with a physical presence in Australia or different obligations are imposed for companies of different sizes or business models, then this would create the same problems of commercial disadvantage and options for circumventing data retention. In this regard, we note the powers in the United Kingdom Government's Data Retention and Investigatory Powers Act 2014, which include extra-territorial powers to capture companies outside the United Kingdom's geographic jurisdiction who provide services to their citizens.

6. **Security implications**

Just as telecommunications data is useful for agencies in protecting public safety, it is highly valuable for individuals and groups involved in cyber-crime or other anti-social activities.

Australian businesses are already facing a growing security threat from external actors seeking to gain unauthorised access to their customer data. By increasing the amount of data we collect on our customers and the length of time we need to keep it for, the proposed scheme will mean Telstra will need to take additional steps to secure our customer data. This would be consistent with our

commitment to customers to keep their data secure, as well as our legal obligations to protect personal information from misuse and unauthorised access or disclosure.

As one of the leading providers of telecommunications security services with a strong track record in protecting customer data from cyber-security threats we are well placed to implement these additional security measures, but this will contribute to the overall cost impact on our business.

7. Oversight and scope limits

The use of telecommunications data by agencies has been the subject of significant public commentary in recent years and the proposed data retention regime has created concern for some of our customers. To help build community confidence and trust in the system we would support oversight mechanisms to ensure agencies are acting appropriately, both in accessing data, storing the data and in implementing any changes to the data set.

In terms of limiting the scope of the Data Retention Bill itself, one important step the Government is proposing is to circumscribe which agencies have the ability to access the data that is to be retained. Currently, a wide array of organisations have access to telecommunications data, extending beyond the police and security agencies to groups such as local councils, taxi regulators and the RSPCA. In our experience, many customers find it difficult to accept that these bodies should have access to their historical customer data.

To address this concern and to limit the ongoing compliance burden of meeting requests for data from these organisations, we support the proposal to limit access to the data associated with the Data Retention Bill to agencies involved in criminal and national security investigations. However, we note that as a result of the proposed amendments to the Telecommunications (Interception and Access) Act 1979, there is now uncertainty as to whether these organisations can revert to using coercive notice to produce or investigatory powers (provided to these bodies under other State or Commonwealth legislation) to access this data. We would recommend additional wording be included in the legislation to ensure there is no back door for these organisations to get access to retained data under other pieces of legislation.

Another measure that could be considered is to establish some limits on what agencies can do with retained data that has been obtained from telecommunications companies. There may be some community concern if agencies are allowed to retain data indefinitely or for a period longer than necessary to complete an investigation or for intelligence gathering. Obligations on agencies to destroy data they have obtained under the Data Retention Bill would help address these concerns and would be consistent with practices in the United Kingdom and the United States.

In terms of oversight once the Bill is enacted, there is an ongoing role for an independent body to review the agencies use of the data retention regime. This might be a role that can be performed by Inspector-General of Intelligence and Security in relation to the national security agencies, with a similar body providing oversight of the law enforcement agencies.

8. Interaction with the Privacy Act

If compliance with the Bill increases the amount of personally identifiable information we hold about our customers, then it will increase the regulatory burden imposed on industry by the Privacy Act. In this regard, we note the comments by the Privacy Commissioner that the data being retained under the Bill could be considered 'personal information' under the Privacy Act.[2]

On top of our obligation under the Privacy Act to protect against data breaches, the manner in which the data will need to be held to comply with the Bill may mean that Telstra could be required to make this data available to individual customers in response to an access request for personal information. Currently, we comply with this obligation by making available the data held against an individual's

[2] Timothy Pilgrim, Australian Privacy Commissioner, Australian Government's data retention proposal — statement, August 2014

name in our billing and customer management system. If a data retention system is to be created within Telstra and further data is to be held against individual's names or other identifiers that link the retained data to an individual, then we may also make it available upon request to the relevant customers.

Providing this information to customers is not the same as providing information to authorised enforcement agencies and would involve additional costs, for example in verifying a customer's identity and redacting information on incoming calls to protect the privacy of other individuals. There is a fundamental difference between responding to a reasonably precise and limited request from agencies for information to dealing with blanket requests for all personal information about an individual.

The costs associated with the systems, processes and labour, required to verify customer requests and retrieve the relevant data, has not been taken into account by Telstra in determining the cost impacts of the Data Retention Bill. Telstra does have the ability to charge customers for providing access to personal information, but we consider it a real risk that we would not be able to fully recover our costs in light of the Office of the Australian Information Commissioner's (OAIC) Australian Privacy Principles Guidelines on charging for access requests.

The OAIC's guidelines state that charges for access requests by an organisation must not be excessive. Whether a charge is excessive depends on the "nature of the organisation including the organisation's size, resources and functions". This suggests that larger organisations may be expected to bear a significant proportion of these costs. Further, the examples of items set out in the guidelines which can be charged indicate that capital costs cannot be included in such charges and organisations are encouraged to consider "waiving, reducing or sharing any charge that may be imposed, so that the charge is not excessive".

Finally, we also operate under a requirement in the Privacy Act to destroy or de-identify data once no longer required for purposes for which they were collected. This could be interpreted as meaning we are legally required to immediately destroy or make amendments to the data retained under the Bill as soon as the two year retention period has ended thereby creating a further rolling obligation and additional cost on industry unrelated to commercial purposes that we have not yet factored into our assessment of the Bill. To help limit this impact, we believe that if there are to be different data retention periods across technologies as part of this scheme, we would recommend that telecommunication service providers be given the option of retaining data for the longest permitted period without breaching the law.

9. **Court orders**

If enacted, the Data Retention Bill would increase the volume of data we are required to retain and is likely to also raise public awareness of this fact. As a result, we expect to receive an increase in the number of court orders we receive to make customer data available to the courts as part of civil ligation proceedings that otherwise does not involve Telstra. These court orders can already be quite resource intensive to comply with today as they often require the telecommunications company to interpret the data for the courts. Also industry does not have the option of cost recovery on court orders. Telstra recommends that industry be given the ability to recover the costs arising in providing information in response to court orders.

IT'S HOW WE CONNECT

10. **Next steps**

Telstra appreciates the Government's efforts to consult with industry in the development of the Data Retention Bill. The telecommunications sector is highly complex and as this submission outlines, the legislation has many and varied impacts on industry. As such, we believe the Government should commit to a formal ongoing consultation process with industry around the implementation of the Bill and associated regulations. We would recommend the current Data Retention Implementation Working Group, which includes senior representatives of Government and industry, continue for the foreseeable future to provide a forum to address any operational issues that will need to be addressed if and when the Bill is passed.


IT'S HOW
WE CONNECT