TELSTRA CORPORATION LIMITED

Review of the Mandatory Data Retention Regime

Submission to the Parliamentary Joint Committee on Intelligence and Security

26 July 2019

01 Introduction

Telstra appreciates the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (the PJCIS) review of the mandatory data retention regime (**the Regime**). We are a major builder and supplier of telecommunications networks and services, with a large customer base and a long history of providing lawful assistance to national security and law enforcement agencies (the agencies). We, along with other participants in the telecommunications industry, were active participants in the public discussion about the costs and benefits of and, ultimately, the requirements and funding of the Regime through various consultations and the Government's Data Retention Implementation Working Group.

Lawful access to telecommunications data is an important tool for the agencies that helps protect lives and solve serious crimes in this country. At the same time, an appropriate balance needs to be struck between delivering safety and law enforcement to protect the public, and meeting Australian consumers' expectations of privacy and minimising the regulatory burden imposed on industry.

Our submission identifies a number of areas where we believe there is room for improvement in the Regime, including:

- Limiting the ability of non-law enforcement agencies to use s.280 of the *Telecommunications Act 1997*[1] to access telecommunications data without a warrant.
- Reducing complexity for telecommunications companies when assessing whether it is permissible to release certain categories of data.
- Consideration of whether there is a need for industry wide exemptions for Internet of Things (IoT) devices.

Our submission concludes by observing that the Regime has benefited from collaboration between government and industry during development and the early stages of implementation, particularly with respect to establishing and maintaining a stable data set since the Regime was established in 2015.

02 Balancing access to the Regime with customer privacy

When the Regime was introduced in 2015, it was recognised that with the evolving nature of smart phone technology and usage, access to a person's telecommunications data had the potential to provide more far-reaching insight into the activities of a person and those they communicate with. To mitigate the risk of unnecessary privacy intrusions, a number of controls to limit access to the data were put in place, including but not limited to:

- The number and nature of agencies intended to be able to access telecommunications data under the Regime was limited to criminal law-enforcement agencies listed under section 110A of the TIA Act.[2]

[1] Section 280(1)(b) of the *Telecommunications Act 1997*, provides a disclosure or use is not prohibited if the use or disclosure is required or authorised by or under law.

[2] https://www.legislation.gov.au/Details/C2015A00039

- Access was for serious criminal activity and national security risks only.[3]

- Authorising officers are required to consider whether any interference with the privacy of any person or persons that may result from disclosure were justifiable having regard to the likely relevance and usefulness of the data and the reason the disclosure or use is proposed to be authorised.[4]

It is questionable whether these controls are operating as effective as intended. We agree with and support the Communications Alliance submission to this inquiry which notes that in November 2018, in response to a request received from the PJCIS, it provided a list of "… *approximately 60 entities that had sought data using means outside the provisions of the data retention legislation*." While the issues these agencies and bodies are dealing with are undoubtedly significant in their own domain, they may not fall into the category of "serious criminal activity or national security". These agencies and bodies have relied on s.280 of the Telecommunications Act to access telecommunications data, thereby circumventing the intended restriction and avoiding assessment of whether disclosure is justifiable and proportionate.

There is a risk this type of access to telecommunications data could erode public trust in the Regime and undermine the relationship we have with our customers in relation to protection of their privacy. In some cases, these agencies and bodies are also not contributing to the cost recovery of the Regime.

Our proposed solution is for all organisations accessing telecommunications data (even if they are not an identified law enforcement agency) to be required to follow the process set out for enforcement agencies in Division 4 of Chapter 4 of the TIA Act. While this approach would not limit the non-law enforcement agencies from accessing telecommunications data, it would have three benefits:

- It would mean carriers and carriage service providers would not bear the burden to check and verify the coercive powers of every State, Territory or Commonwealth agency/department requesting data.

- It would require the authorising officer to consider whether access to the data is justifiable and proportionate, etc.

- It would provide clarity that all entities seeking telecommunications data are captured under the standard cost recovery system of the Regime, which may also encourage them to carefully consider the amount and scope of data required.

For clarity, we are not proposing these agencies be added as law enforcement agencies; rather, they be required to follow the same process, making them subject to the same obligations and constraints (test of proportionality, contribution to costs, etc.) as the listed law enforcement agencies.

Another area where the balance between access to the Regime and consumer privacy/protection could be improved is in relation to the amount and type of data requested. In our experience, non-enforcement agencies and bodies often request large amounts of data and are sometimes not able to properly interpret the data provided. Requiring all agencies and bodies requesting access to telecommunications data to follow the process set out in Division 4 of Chapter 4 of the TIA Act, including meeting the cost of providing the data, might also provide an incentive for those agencies to carefully consider the amount and scope of data requested. In addition to the obvious resource burden imposed on the service provider, supply of irrelevant or unnecessary data further undermines public trust in the Regime.

---

3 https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-retention-obligations

4 Section 180F of the *Telecommunications (Interception and Access) Act 1979*.

Under the Regime service providers are required to encrypt and securely protect retained data.[5] We are concerned that agencies and bodies not listed in s.110A of the TIA Act may not have sufficiently strong security measures to protect received data. Accordingly, we believe there is a need for the introduction of appropriate oversight mechanisms to ensure measures are in place to securely protect disclosed data and to control who can/can't access the data.

03 Complexities in assessing whether it is permissible to release certain categories of data

One of the privacy protections introduced by the Regime was to limit disclosures of telecommunications data when held solely for the purpose of the Regime. However, this limitation is overly complicated as providers need to assess whether some or all of the data requested under any subpoena, notice to produce or court order is (1) being held solely for purposes under the Regime; and (2) being requested in connection with a civil proceeding, in order to determine if any or all of the data can be provided. We agree with the Communications Alliance submission on this point, which provides greater detail on the challenges carriers and carriage service providers face in assessing whether it is permissible to release data, and we propose that the PJCIS should give consideration to this matter in the current review. We support the Communications Alliance's proposed approach to solving this concern:

> *As an industry, C/CSPs would like to see a consistent, transparent and practical legal process put in place that will enable C/CSPs to respond to lawful requests from a genuinely limited number of agencies and courts, and in a manner that protects a customer's personal information and enables C/CSPs to recover their costs, including from civil litigants, and excludes liability in all cases of disclosure.*[6]

Ideally, we would like to see the need for this assessment by service providers removed. This could be done in conjunction with the number of Government authorities being able to obtain this data being reduced and requiring all authorities to follow the process set out in Division 4 of Chapter 4 of the TIA Act to obtain telecommunications data. As discussed previously, the requirement to consider privacy and the cost recovery provisions will likely reduce the scope of data being sought.

04 Retention requirements for 'Internet of Things devices

There are already a vast number of IoT devices deployed and operating and the number of connected 'things' is forecast to exponentially increase over the next few years as new technologies are rolled out.[7] However, there appears to have been little consideration about the costs and benefits of requiring carriers and carriage service providers to store the mandatory telecommunications data for these devices. We believe consideration should be given to providing industry wide exemptions to certain IoT technologies or use-cases. For example, it seems unlikely that the timing and length of data sessions from a smart meter which provides throughput or output measures at regular intervals would provide useful information to the listed law-enforcement agencies. Importantly, if exemptions are identified, they

[6] Communications Alliance, *Submission to the Parliamentary Joint Committee on Intelligence and Security review of review of the mandatory data retention regime*, 12 July 2019, p. 7.
[7] Ericsson forecast the number of 'connected cellular' Internet of Things devices will increase from less than one billion in 2018 to more than four billion in 2024.

should be applied uniformly across industry, such that any service provider who provides that service is exempt from the Regime.

05 The regime benefits from stability and industry participation in its design

The Regime has benefited from collaboration between government and industry during development and the early stages of implementation particularly with respect to establishing and maintaining a stable data set since the Regime was established in 2015. Any changes to the Regime, including the required data set, need to be subject to detailed consultation with industry to ensure the benefits from change are realised and are greater than the cost to industry of implementing the change.

Changes to our systems and processes that may result from decisions to address the concerns outlined above, or made by others, could create significant cost to industry, through further capital investment in systems, or changes to processes that are now familiar and well-tuned within our organisation.

In balancing the need of providing lawful assistance to national security and law enforcement agencies with the interests of taxpayers/consumers, it is important to take a pragmatic view of the cost and difficulty of implementing changes to the Regime to ensure the balance is struck in a manner that meets the cost/benefit expectations of the Australian society.