3 February 2017

Ms Jessica Robinson
A/g Assistant Secretary
Infrastructure Security and Resilience Branch
Department of Communications and the Arts

Ms Anne Sheehan
Assistant Secretary
Communications Security Branch
Attorney-General's Department

Email: communicationssecurity@ag.gov.au

Dear Ms Robinson and Ms Sheehan,

Consultation Paper – Access to Retained Data in Civil Proceedings.

Telstra welcomes the opportunity to provide comments on the DoCA and AGD's "Consultation Paper – Access to Retained Data in Civil Proceedings" (**the Paper**).

We acknowledge the efforts of the Federal Government in constructing a regulatory framework which enables the lawful access to retained telecommunications data (**retained data**). We recognise and support the accountability that Carriers/Carriage Service Providers (**C/CSPs**) have to ensure the security and protection of the telecommunications information they are required to retain under the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**) and the Telecommunications Act 1997 (**Telco Act**). We also recognise that parties to civil litigation may wish to be able to access retained data for the purpose of such proceedings. This response outlines our views on the practical issues that C/CSPs will face in complying with the current prohibition on providing access to retained data in civil proceedings and makes some suggestions on options for addressing these issues.

1. Prohibition of disclosing retained data for civil proceedings

1.1 Introduction

The introductory letter attached to the Paper states that:-

> "*From 13 April, 2017, telecommunications companies will be prohibited from disclosing telecommunications data that they retain solely for the purpose of complying with their data retention obligations under the Act in response to subpoenas, notices of disclosure or other court orders in conjunction with civil proceedings.*"

This approach to prohibiting access to retained data after the 13 April 2017 raises a number of practical compliance issues for C/CSP's. This is because it is not always straightforward to determine what data is retained "solely for the purpose of complying with the data retention obligations". To determine if the data is retained solely for the purpose of data retention obligations will require C/CSPs for each subpoena, notice of disclosure or other court order to:

- Determine the parties that are engaged in civil litigation;

- Determine what data is sought, and whether that data is retained 'solely for data retention purposes' or whether it is retained for other business purposes associated with the C/CSP's business. This may be a complex question of fact and will add to the already significant costs of complying with the data retention regime; and

- Make or defend an application to the court, supported by evidence, where they are unable to respond to a subpoena, or other court orders because the data sought is retained solely for the purpose of the data retention regime.

If the Federal Government was considering amending the TIA Act, some alternatives to the current prohibition include:

- Permitting access to any telecommunications data in civil proceedings with leave of the court, where the party requesting the information specifies what information is required and why that information is of evidentiary value in the proceedings. The application could set out how the privacy of any individual's data so obtained would be protected; or

- Remove the prohibition on access to data retained solely for the purpose of complying with data retention obligations. This would mean that parties to civil litigation could continue to request data required from non-party C/CSPs in civil litigation. The current subpoena, court orders and other notices of disclosure are supervised by the court in a range of civil litigation, including in relation to sensitive data that is relevant in any court proceedings. This approach has the advantage of enabling access to relevant material required for civil litigation, and does not require C/CSPs to make determinations about what information is required to be retained solely for data retention obligations. While more data will be retained, in some cases for longer periods than is the currently the case, the fundamental question in any civil litigation is how does that data advance the civil case. In civil cases we think that it is likely that data relating to, say location, is less likely to be of interest than such data is for law enforcement purposes. A court is likely to be in a better position to determine the probative value of any data requested on a case by case basis. The court supervision of the subpoena processes would enable the right balance between the legitimate needs of parties to obtain information relevant for court proceedings, and protecting an individual's privacy.

The preferred outcome would be a continuation of disclosure rules that provide the Court with the power to decide when to allow access to retained data in civil proceedings independent of the civil matter under consideration.

1.2 Data Retention and civil proceedings – implications of current regime

The TIA Act does not stipulate how a C/CSP must technically comply with the requirements of the TIA Act. In some cases C/CSPs may opt to execute their DRIP (Data Retention Implementation Plans) which indicates that they will ingest telecommunications data that was retained for business purposes into a centralised secure data retention store separate from existing customer IT systems and/or developed new systems that deliver the data required under s187AA of the TIA Act to a centralised secure data retention store. To comply C/CSPs will need to determine if the requested data has been ingested or not to determine the legal status of the data and then if it can be made available or not.

This will create uncertainty for staff in having to differentiate between what telecommunications data is retained for the purposes of s187AA of the TIA Act and what data is retained for other business purposes. This may be the case particularly if C/CSPs are put in a position where they have to determine at what point in their systems the data retained is in

compliance with the TIA Act or whether the data is retained solely for day-to-day business purposes. This added logistical hurdle adds costs to the process of compliance. The differences in approach may also make it complicated for parties to litigation to know what data they will be permitted to have access to.

1.3 Increased uncertainty for C/CSPs

In addition the above, a further potential issue with the proposal in the Paper is that it may put C/CSPs in a position where they will need to query whether or not the request for data is for a civil proceeding or not. Again, this would inevitably introduce the risk of potential inadvertent disclosures and will result in uncertainty for C/CSPs, leading to a situation that may require C/CSPs to undertake a legal analysis of each request which is received prior to releasing (or declining to release) the requested data. This will result in a more complex decision making processes resulting in further additional delays, the involvement of additional stakeholders and resources which will the raise cost of compliance.

We would therefore suggest that the authorisation by or under law as to when a C/CSP can release retained data is made very clear and transparent under any proposed amendments. We do not think C/CSPs should be placed in a position where they are required to make a judgement call on every lawful request as whether or not to release retained data or distinguish between retained or business data. This will only increase the regulatory and cost burdens on society which is already high in this regard.

1.4 Liability for acts done or omitted in good faith

In respect of the release of retained data, C/CSPs should not be held liable in relation to any retained data released or withheld in relation to a request in a civil proceeding. Currently, s313(5) and s313(6) of the Telco Act limit a C/CSP's liability (their officers, employees and agents) for acts done or omitted in good faith in connection with help that is reasonably necessary for the enforcement of criminal law and other security related activities. However, these protections do not currently apply to assistance with civil proceedings and would need to be replicated for any assistance supplied in civil proceeding especially considering the increased risk associated with the added complicity and logistical requirements identified above

1.5 Cost Recovery

If retained data is made accessible in civil proceedings and was extended through exclusions to s280 of the Telco Act (or any other instrument), we must be able to recover our costs. This could be done in a similar manner to the fees levied on agencies for the provision of information currently retained. Currently, conduct money is provided when telecommunications data is released in response to a subpoena. Rarely does this cover the costs of producing the relevant material (where the subpoena is for production of documents) or the costs of providing witnesses to court where the subpoena requires us to provide oral evidence. The advantage of system of fees is that it would be clear to parties in civil litigation the costs likely to be incurred for such data requests.

2. Responses to questions raised in the Paper

1. ***In what circumstances do parties to civil proceedings currently request access to telecommunications data in the data set outlined in section 187AA of the TIA Act […]?***

   We are unable to provide information in response to this question as parties involved in civil proceedings do not inform us as to what the circumstances are of the civil proceeding. We currently receive on average of 500 to 600 requests for

telecommunications data each year by court order. These are set out in our yearly 'Transparency at Telstra' Report available at https://www.telstra.com.au/privacy/transparency.

2. ***What, if any, impact would there be on civil proceedings if parties were unable to access the telecommunications data set as outlined in section 187AA of the TIA Act?***

   Our understanding of the Paper is that the review aims to consider a prohibition on access to currently accessible retained data after 13 April 2017. In the context of the Paper, this question is confusing: if data has been retained for other business purposes and not for compliance with section 187AA, it is accessible in civil proceedings. If not and it is retained solely for data retention regime purposes, it is not accessible in civil proceedings (after 13 April 2017).

3. ***Are there particular kinds of civil proceedings or circumstances in which the prohibition in section 280(1B) of the Telecommunications Act 1997 should not apply?***

   This is a matter for the parties to the civil litigation proceeding.

Telstra is keen to continue to participate in ongoing discussions with your Departments and relevant agencies to discuss our submission and help reach practical resolution to the issues that have been raised as part of this consultation process.

Please do not hesitate to contact Michael Ryan on (07) 3455 0370 or by email at michael.j.ryan@team.telstra.com if you have any queries about our comments in this submission.

Yours sincerely,

Jane van Beelen
Executive Director – Regulatory Affairs
Corporate Affairs

jane.vanBeelen@team.telstra.com