27 January 2017

As email to: **CommunicationsSecurity@ag.gov.au**

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

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

RE: Consultation on access to retained telecommunications data in civil proceedings

Dear Anne, Dear Jessica,

Thank you for giving us the opportunity to provide feedback to the Minister for Communications and the Arts (Department) and the Attorney-General's review of access to retained telecommunications data by parties in civil proceedings.

The Consultation Paper poses three specific questions which we address below:

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 […]?*

There is no industry-wide register of subpoenas and other civil orders requiring the delivery of information to litigants in civil proceedings. Each of the major carriers receives a regular flow of requests for information from a large number of lawyers acting for civil litigants and Government agencies. There is also a regular flow of telephone enquiries regarding what information might be available and how to request it. Many requests for civil information relate to information that C/CSPs do not have, do not have at the time of the request or are unable to provide.

There are significant costs in dealing with the inquiries and the consideration and investigation process. (See our comments further below.)

Major C/CSPs have provided information about sources of requests for data to the Department and the Attorney-General in mid-2016 on a confidential basis. It is recommended that C/CSPs be approached directly and individually by the Department/Attorney-General should they wish to receive information about requests from civil litigants. However, based on the type of data usually requested under a civil subpoena, it appears that currently civil litigants are not usually seeking production of detailed communications data that C/CSPs will be retaining after the completion of the Implementation Phase of the DR regime. However, C/CSPs are unable to judge whether such data would be sought more often in the future.

If data that is also being retained under s187AA of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) is being retained for purposes other than compliance with the data retention (DR) regime (even if, in addition to its other purposes, it continues to be stored under

the DR regime), then these data may be accessed in civil proceedings under subpoena or a court order.

In practice this means that any data retained prior to completion of the Implementation Phase of the DR regime (13 April 2017) is accessible in civil proceedings. Such data may have been retained for varying lengths of time depending on the individual C/CSP's internal requirements and/or other legal obligations requiring the storage (and subsequent deletion) of data.

Data retained after completion of the Implementation Phase of the DR regime is only accessible if it has been retained for purposes other than compliance with the DR regime. It is important to note that these data will only be accessible in civil proceedings for the period that the data has been retained for such other purposes which may be more or less than the two-year retention period of the DR regime. As an example, if data required to be retained under the DR regime for two years has only been retained for six months for other purposes, then the data will not be available for the remaining eighteen months during which it has been retained solely for the purpose of complying with the DR regime.

While Industry does not seek to provide an opinion on privacy or civil justice implications of an extended access regime, we would like to note the following: As Industry understands it, a civil court registry will usually issue a subpoena at the request of a party to the proceedings without the registry having regard to the reasonableness or scope of the request or the privacy or confidentiality impacts of disclosure of the data being sought. A subpoena may seek production of data about any person, including persons who are not a party to the proceedings. This means that the subpoena process allows a party to civil proceedings to obtain access to data about a person who is not a party to the proceedings and who may only be vaguely related to the proceedings. In addition, only the parties to the proceedings or the recipient of the subpoena (in this case the C/CSP who responded to the subpoena) would have notice that the data have been requested and are being provided to the court for production. A person who is not a party to the proceedings and whose records are being produced by the C/CSP would usually not be present at the subpoena return date and would not have an opportunity to argue against production of the data relating to them. Once the court has received the data, it may be very difficult to control the use or access to the data.

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?*

In the context of the Consultation Paper, this question is confusing: if data has been retained for purposes other than compliance with the DR regime, it is accessible in civil proceedings. If not and it is retained solely for DR purposes, it is not accessible in civil proceedings (as of 13 April 2017). Accordingly, it is not necessarily the case that parties in civil proceedings are currently able to access the communications data set as outlined in section 187AA of the TIA Act.

Our understanding of the Consultation Paper is that the review will consider an extension of access to data currently inaccessible post 13 April 2017, rather than reducing access to currently accessible data (i.e. data retained for other purposes).

However, should access to communications data by civil litigants be further restricted, we would expect a greater level of privacy for individuals. As already indicated in the Consultation Paper, such improved privacy may operate as an impediment to civil justice.

The trade-off between the two appears to be an overarching question that needs to be dealt with by legislation when considering the issue of access to metadata in providing assistance to

civil justice rather than leaving it up to C/CSPs to determine who can obtain access to retained data post 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?*

While individual members of our organisations may have an opinion on this matter, the question might be best answered by civil justice and privacy experts.

However, given that the telecommunications industry would be required to assist with the execution of any extended access regime, it is important to bear the following in mind:

1. Currently, in relation to requests for data from law enforcement and national security agencies C/CSPs are required to carefully distinguish whether a requesting agency has the required powers (i.e. coercive 'powers to produce' under their own legislation) and, consequently, whether data ought to be released. This already increases uncertainty and liability issues for C/CSPs. (This separate but related issue has been brought to the Department's/Attorney-General's attention in the past and appears to be under internal investigation. Please refer to the section *Access to communications data pursuant to s280 of the Act remains problematic* further below.)

   The situation in relation to requests for information in civil proceedings is also unnecessarily complicated. It does not make sense that some information is provided while other information is not, based on a potentially difficult and complex investigation of how and for what purpose the information was kept or used prior to 13 April 2017.

   Any further broadening of the situation through additional uncertainty regarding the legal status of the data (whether or not it should properly be provided) and under what law it is requested to be made available would not be acceptable.

   The TIA Act did not stipulate how C/CSPs must comply with the TIA Act. However, in some cases C/CSPs have complied with their Data Retention Implementation Plan (DRIP) by ingesting communications data into a centralised secure data retention system (that complies with the TIA Act) from existing customer IT systems and/or developed new systems that deliver the data outlined in s187AA of the TIA Act. In this particular situation, C/CSPs will need to determine if the requested data has been ingested or not to determine the legal status of the data and whether it can be made available.

   It appears likely that a narrow and specific extension of the accessibility to data only for certain kinds of civil proceedings would result in further uncertainty for C/CSPs and indeed lead to a situation that would require C/CSPs to undertake legal analysis for each request to disclose data prior to releasing (or declining to release) the requested data for civil proceedings.

   Therefore, many C/CSPs tend to prefer an 'all or nothing' approach to this matter, i.e. either a continuation of the currently existing disclosure rules (albeit with a clearer, more limited regime of which agencies can lawfully access retained metadata or other data) or a regime that allows access to all retained data in civil proceedings independent of the civil matter under consideration. In any case, and including in case of an extended access regime, clear regulations are required as to which agencies and courts will be able to request data and whether these data comprise all data retained by C/CSPs, including detailed metadata. In this context issues around the reimbursement of costs

associated with such data requests urgently need to be addressed. (See comments further below.)

2. C/CSPs must not be held liable in relation to any data released or withheld in relation to civil proceedings. Currently, s313(5) and s313(6) of the *Telecommunications Act 1997* (Act) afford liability protection to providers, 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.

   These protections do not apply to assistance with civil proceedings and would need to be mirrored for any assistance supplied in those cases. We note that such liability protections in civil proceedings are required independent of an extended scope of data accessible in civil proceedings. C/CSPs also request that data made available in relation to civil proceedings (and the fact that data has been disclosed) be inadmissible to any other proceedings but the specific civil proceeding for which they were sought and made available by C/CSPs. This will increase legal certainty for C/CSPs and, thereby, may assist with a smooth disclosure process.

3. If the scope of the data that is being accessible in civil proceedings were to be extended through exclusions to s280 of the Act (or any other instrument), C/CSPs must not bear any additional costs as a result of an increased volume of requests or any other consequences of these changes. Any expanded scope of data access will result in substantial additional costs, including additional staff required to handle an increased volume or higher complexity of requests and/or capital expenditure required to update or develop databases and interrogation tools etc.

   It should be noted that C/CSPs have difficulty seeking recovery of costs for complying with subpoenas. Pursuant to s314(2) of the Act, C/CSPs may recover the cost of assisting an agency authorised to request such assistance under the DR regime. However, this provision does not extend to responding to subpoenas from other agencies.

   In the case of civil requests there is generally a right of cost recovery available to C/CSPs associated with the civil court system. Unfortunately, the compensation offered is often inadequate and/or not paid when due. Research indicates that approximately 40% of invoices issued seeking payment of reasonable costs of complying with a subpoena are not paid. The process places an onerous financial burden on C/CSPs to comply with civil subpoenas. The amounts involved are usually small and do not justify the costs associated with pursuing recovery at law. If Government decided to increase the scope of data to be made available for use in civil proceedings, C/CSPs request that a mechanism be included for C/CSPs to charge upfront (also see comments below) for the cost of consideration, investigation and, where available, the cost of recovering and delivering the data in response to civil requests. The right of cost recovery should include an ability to recover all capital expenditure necessary to put in place appropriate systems and procedures. Such an approach to cost recovery would help ensure that the information is requested only where genuinely required and that the burden of complying with the expanded duty does not operate as a burden on C/CSPs' customers.

4. Any reimbursement of costs (e.g. via a fee schedule) ought to be upfront and independent of the timing of the financial settlement of the case as it is common practice with many other services provided in the private or public economy. This could be done in a similar manner to the fees levied by ASIC for the provision of information on companies listed in their databases. As it stands, already today C/CSPs often have to go

through significant effort to recover their costs for assistance requests. Were the volume of requests for data to increase, such upfront cost recovery would become imperative.

5. If the scope of data accessible in civil proceedings were to be increased, it ought to be clear that dealing with such requests may not be a matter of highest priority for C/CSPs whose staff also deal with important matters of national security and provide assistance to enforcement in criminal proceedings. This means that requests for data in civil proceedings ought to be submitted to C/CSPs with sufficient lead time, e.g. four weeks, and the understanding that national security and criminal matters have a higher priority.

As an industry, C/CSPs would prefer to see a consistent, transparent and practical legal process put in place that will enable C/CSPs to respond to lawful requests from all courts and agencies in a manner that protects a customer's personal information and enables C/CSPs to recover their costs, including from civil litigants.

Access to communications data pursuant to s280 of the Act remains problematic:

In the past, Industry has raised concerns with the Department/Attorney-General regarding the current rules around agencies who have access to metadata pursuant to s280 of the Act and the recovery of costs associated with access requests.

As this issue is likely to be exacerbated were the access regime to be extended, we would like to reiterate some of these concerns.

The power to request information under the Act was withdrawn from a number of agencies with the introduction of the DR regime which included the introduction of the definition of Enforcement Agency.

Pursuant to s280(1)(b) of the Act, C/CSPs must respond to information requests where "the disclosure or use is required or authorised by or under law". Several agencies that were excluded from the list of Enforcement Agencies with the introduction of the DR regime are now simply relying on powers in their own statutes to request data. Such agencies include local councils (who request access to data to manage minor traffic offences, unlawful removal of trees, illegal rubbish dumping and billposters), the RSPCA, the Environment Protection Authority and state coroners, to name a few. The use of these other powers to access communications data appears to circumvent protections in the Act and TIA Act. For example, the following sections of the TIA Act would not apply to agencies using their own powers to request communications data:

- 178(3): The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law.
- 180F: Authorised officers to consider privacy
- 186A: Obligation to keep records

In addition, Industry considers that, as C/CSPs respond to requests for data pursuant to s280 of the Act, s313 and s314 of the Act ought to apply and Industry ought to be able to recover any costs associated with the provision of the assistance that has been given. This is currently in dispute with many agencies who rely on powers outside of the Act and, consequently, do not reimburse C/CSPs for the costs incurred.

We invite the Department/Attorney-General to clarify the legal position on these two matters.

We also note that any considerations around the availability and accessibility of data ought to take into account the Productivity Commission's Draft Report *Data Availability and Use*.

Please contact us if you have further questions or would like to discuss.

Yours sincerely,

John Stanton
Chief Executive Officer
Communications Alliance

Chris Althaus
Chief Executive Officer
Australian Mobile Telecommunications Association