COMMUNICATIONS
ALLIANCE LTD

Communications Alliance Submission

to the

Parliamentary Joint Committee on Intelligence and Security (PJCIS)

Review of the mandatory data retention regime

12 July 2019

Page intentionally left blank.

Introduction

Communications Alliance welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the mandatory data retention regime (DR Regime).

Communications Alliance and its Members support the objectives of the DR Regime and were heavily engaged with the Government and, in particular, the Department of the Attorney General, throughout 2014, in an attempt to refine and improve successive exposure drafts of the data retention legislation that was eventually passed by both Houses of Parliament in March 2015.

Given the significant investments made by industry in systems and processes to comply with the DR regime, there is value in retaining stability in the legislative framework over time. Nonetheless, it is timely and appropriate that the DR Regime be reviewed in light of the experience of several years of its operation, given the importance from security, from privacy and from industry/government efficiency perspectives, of having data retention provisions operate as effectively as possible.

This submission highlights a number of areas in which industry believes the DR Regime requires improvement.

These areas include:

- addressing the unintended consequence of a loophole that allows scores of agencies that were not supposed to be able to access metadata on a warrantless basis, to do so;
- the complexities that the legislation presents for carriage service providers (CSPs) as they try to assess whether it is permissible to release certain categories of requested data;
- questions as to whether it is appropriate for metadata to be release for use in civil cases – in some circumstances up to 7 years after that data was first collected;
- concerns about Agencies repeatedly failing to meet their reporting requirements under the legislation, thereby reducing the intended transparency around the data retention arrangements;
- whether the two-year mandatory duration period is appropriate, in light of the experience of the usage of the DR Regime since the legislation first became law; and
- concerns about the appropriateness or otherwise of the current authorisation threshold.

Some of the experiences with the DR Regime have also drawn industry back to the question of the long-overdue need for a thorough revision of the Telecommunications (Interception and Access) Act 1979. In December 2013, the Senate referred this matter to the Legal and Constitutional Affairs Reference Committee, which reported that it received: "much evidence highlighting the need for urgent and comprehensive reform of the (Act)".

Industry has worked hard to comply with the DR Regime and to continue its long and commendable record of cooperation with police and security agencies on law enforcement matters.

Compliance has not, however, been without significant financial cost to industry – and therefore to consumers also.

The initial capital costs incurred by industry to meet the requirements of the regime were partially – but not fully – met via grants from Government. As has been highlighted in information presented to the committee, industry has incurred a net cost to meet its

obligations under the regime of at least $171m over a four year period, despite cost-recovery mechanisms being in place.

We look forward to supporting the Committee's work during this review.

About Communications Alliance

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

Bodies/agencies with access to telecommunications data

The general public (to the extent it is informed about these matters) and also experts, often mistakenly believe that the telecommunications data of ordinary Australian people can be accessed, without a warrant, by only a very limited number of 22 law enforcement and security agencies. The website[1] of the Department of Home Affairs lists 14 agencies (police forces of states are listed as one agency) as the only agencies that have access to telecommunications data on a warrantless basis.

With the introduction of the Data Retention Regime, it was recognised that telecommunications data has the capacity to reveal far-reaching information about a specific person and about other individuals communicating with that person. Consequently, the legislation sought to limit the number of agencies that can request warrantless access to such data. The previous power to request such telecommunications data using the *Telecommunications (Interception and Access) Act 1979* (TIA Act) was withdrawn from a number of agencies when the new the Regime was created, through the introduction of a definition of Criminal Law-Enforcement Agency in s110A of the TIA Act.

After the legislation became law, however, Industry raised concerns on a number of occasions with various Government Departments and the PJCIS regarding the circumvention of the s110A restrictions by bodies/agencies that continued to seek access to telecommunications data outside the framework of the TIA Act, by requesting disclosure of such data pursuant to s280 of the *Telecommunications Act 1997* (Telco Act).

Pursuant to s280(1)(b) of the Telco Act, Carriers/Carriage Service Providers (C/CSPs) must respond to information requests where "the disclosure or use is required or authorised by or under law". Several bodies/agencies that were excluded from the list of Criminal Law-Enforcement Agencies with the introduction of the data retention regime are now simply relying on powers in their own statutes to request data. Such bodies/agencies include local councils (who request access to data to, among other things, manage traffic offences, unlawful removal of trees, illegal rubbish dumping and billposters). The RSPCA, the Environment Protection Authority and state coroners are other examples of entities that have managed to subvert the intended scope of the legislation.

The Government's view, as stated in the Telecommunication (Interception and Access) Annual report, 2016-17 (DoHA) was that following the introduction of the DR Regime, the number of agencies accessing telecommunications data fell from 63 to 20 agencies in the reporting periods 2015-16 and 2016-17 respectively[2],

This is demonstrably not the case.

In November 2018, in response to a request received from the PJCIS during its Inquiry into the Assistance and Access legislation, Communications Alliance supplied a list (compiled via our Carrier members) of agencies/departments/entities that had sought access to warrantless telecommunications data since the passage of the data retention legislation. This list included approximately 60 entities that had sought data using means outside the provisions of the data retention legislation

This list is at Attachment A. Also at Attachment A is a non-exhaustive list of a further 27 entities, also not authorised under the data retention legislation, that have sought access to telecommunications data since November 2018. The most recent list is also diverse, including bodies representing veterinarians, the fishing industry, mining industry, child protection interests, regulators, local councils and more.

[1] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-retention-obligations
[2] p. VI, TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979 Annual Report 2016–17, Department of Home Affairs

In our view these lists demonstrate that not only is the circumvention of the DR Regime by entities outside the 'authorised 22' a serious and persistent phenomenon; it is a problem that continues to grow in magnitude.

The use of these other powers to access telecommunications data appears to override the intended protections in the Telco Act and TIA Act. For example, the following sections of the TIA Act do not apply to bodies/agencies using their own powers to request communications data:

- 180(4): The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the investigation of: (a) a serious offence; or (b) an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years. (for prospective data);
- 180F: Authorised officers to consider privacy;
- 186: Report to Minister and reporting to Parliament; and
- 186A: Obligation to keep records

This extended access to telecommunications data leads not only to the erosion of the protections designed to be afforded to telecommunications data on the basis of the recognition of the data's potential to infringe the privacy of individuals. It also has cost implications for C/CSPs. Industry considers that s313 and s314 of the Telco Act, which provide for the reimbursement of costs, ought to apply and Industry ought to be able to recover any costs associated with the provision of the assistance that has been given pursuant to s280 of the Telco Act. This is currently in dispute with many bodies/agencies who rely on powers outside of the Telco Act and, consequently, do not reimburse C/CSPs for the costs incurred.

Some CSPs also report that agencies, departments and entities that are not officially authorised to request warrantless telecommunications data – but do so – often are unable to interpret the data they have received. They then take up more of the CSPs' time to explain the data, then sometimes also call on CSPs to appear in court on relatively minor issues as expert technical witnesses. These additional impositions on the time and resources of CSPs also, of course, go unreimbursed.

Importantly, the dual access regime also means that, in relation to requests for data from bodies/agencies, C/CSPs are required to carefully distinguish whether a requesting body/agency has the required powers (i.e. coercive 'powers to produce' under their own legislation) and, consequently, whether data ought to be released. This increases uncertainty and liability issues for C/CSPs.

This loophole for accessing sensitive telecommunications data ought to be closed through an amendment of s280 of the Telco Act. We also note additional complexities around the distinction of the purpose for which data is stored and subsequently sought that are introduced by that section, discussed further below. It should also be noted that other bodies/agencies may also approach a law enforcement agency listed under s110 of the TIA Act to make the authorisation on their behalf.

One option for consideration would be for all organisations accessing telecommunications data (even if they are not an 'enforcement agency') to be required to follow the process in Chapter 4 of the TIA Act. This would have three benefits:

- it would mean service providers would not to check and verify the coercive powers of every agency/department requesting data;
- it would require consideration of whether access is justifiable and proportionate etc; and
- It would bring all entities into coverage of the standard cost recovery regime.

What data can be accessed and for what purpose?

Another common misperception is that telecommunications data can only be accessed for the purpose of investigating serious criminal offences or at least the enforcement of criminal law. This is also not the case. S179 of the TIA Act already allows that authorisations be made for the enforcement of a law imposing a pecuniary penalty or protection of the public revenue. The loophole of s280 of the Telco Act may cast the use of such data even wider.

In addition, we highlight that telecommunications data can also be accessed in civil proceedings as will be discussed below.

Apart from concerns that may arise from a civil liberties perspective regarding the scope of purposes, it is important to highlight that s280 of the Telco Act introduces a number of complexities for C/CSPs in assessing whether the disclosure of requested data is permissible.

If data that is being retained under s187AA of the TIA Act is also being retained for purposes other than compliance with the DR Regime (even if, in addition to its other purposes, it continues to be stored under the DR Regime), then this 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 (defined in s187H(2) TIA Act, i.e. 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 this 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. Equally, if the data is being retained for other purposes for 7 years, then the data would be available for civil proceedings for the entire 7 years.

While Industry does not offer an opinion on privacy or civil justice implications of this access in civil proceedings, 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 incidentally 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.

The situation in relation to requests for information in civil proceedings is 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.

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 should be noted that cost recovery pursuant to s314 of the Telco Act is not available for data disclosed in civil proceedings, and cost recovery through the court system is very slow at best, often does not cover actual expenses and/or is so cumbersome that C/CSPs abandon any efforts of recovery.

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 Telco 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 ought to be mirrored for any assistance supplied in those cases. 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.

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.

Transparency and reporting

S186 of the TIA Act stipulates that law enforcement agencies must provide the Minister "As soon as practicable, and in any event within 3 months, after each 30 June […] a written report that relates to the year ending on that 30 June" which contains (among other things) metrics on the various forms of authorisations made, the offences for which those authorisations were made, the kind of data (as per s187AA(1)) that has been requested and how long such data had been retained at the time of the request. The reports are also to include information about authorisations that were made under a journalist warrant.

S186(3) sets out that the report "be laid before each House of the Parliament within 15 sitting days of that House after the day on which the report was completed." Unfortunately, the subsection fails to provide a clear deadline by which such report must be completed.

S187P specifically addresses reporting on Part 5-1A of the TIA Act (i.e. the Data Retention Act) but again fails to require a clear deadline and instead only requires a report be prepared "as soon as practicable after each 30 June". (Note that this report on Part 5-1A forms part of the report under s186 and, therefore, has the potential to hold up the entire reporting.)

While the information to be reported may benefit from refinement and further additions – such as the inclusion of information on the results derived from the use of the data (e.g. arrests or conviction) as reported for interception warrants – we agree that the reporting as such is integral to ensuring that this far-reaching Regime is functioning as intended, is fit for purpose and subject to scrutiny by Government, the Opposition, Industry, civil society

organisations and the general public. Indeed, the last published report (2016-17) itself notes that "The annual report is an important part of this accountability framework."[3]

Consequently, we wish to record our dismay and objection to the fact that for the past two reporting periods (the periods during which the new DR Regime was in force) it took thirteen and a half months from the end of the relevant financial year to table these important reports in the House of Representatives (14 August 2017 for the 2015-16 report, 15 August 2018 for the 2016-17 report).

We are even more perplexed that the report for the 2017-18 reporting period – the only full reporting period outside the Implementation Phase – has (as at 12 July 2019) still not been tabled and published, even though the PJCIS was due to commence its statutory review by 13 April 2019 (note the caretaker period) and, indeed, has requested submissions be made prior to the report being published. We expressly note that this is not a criticism of the PJCIS nor its timing of the inquiry process.

As an aside we also point out that Industry faces numerous, often very onerous, reporting requirements, tied to tight deadlines. For example, C/CSPs must provide the Australian Communications and Media Authority (ACMA) with extensive data sets on complaints and subscriber numbers, which are difficult to extract from various internal systems, within 30 days of the end of the (quarterly) reporting period.

Therefore, we request that the legislation be revised to require that the reports pursuant to s186 (and 187P) of the TIA Act be tabled and published within three months of the end of the reporting period, i.e. by 30 September.

It is also important to note that the report will only include information about requests made pursuant to the TIA Act. Requests made through use of s280 of the Telco Act will go unreported, thereby leading to a further gap in transparency.

Retention period

Table 38 of the report highlights that the vast majority of requests for existing data, i.e. 94% of all requests, was made for data that had been, at the time, retained by the C/CSP for 12 months or less, with 79% of requests pertaining to data that was only retained for 3 months or less.[4] This demonstrates that the approach taken by the Australian Government when drafting (and passing into law) the DR Regime was unnecessarily wide – an approach that came at the expense of C/CSPs which only saw a fraction of their implementation costs reimbursed by Government. As already argued in 2015, a retention period of 24 months is also out of step with almost any other jurisdiction that has implemented (or attempted to do so) a DR Regime. For example, the European Union Directive on Data Retention (in December 2016 largely declared unconstitutional by the Court of Justice of the European Union (CJEU)) prescribed a minimum retention period of 6 months with a maximum(!) retention period of 24 months.

While significant investments into storage capabilities have already been made, Industry considers that a shorter retention period would be more appropriate, also with view to a potential increase in telecommunications data that may be generated as technologies evolve. We note that such a change to a shorter period ought not affect data that has already been retained under currently effective legislation.

[3] p. VI, TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979 Annual Report 2016–17, Department of Home Affairs
[4] p. 49 TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979 Annual Report 2016–17, Department of Home Affairs

Authorisation threshold

As discussed extensively in public debate, telecommunications data can provide very detailed and intrusive information about a targeted individual and, importantly, also about an individual that is not subject of an investigation but has communicated with the subject of the investigation. In many instances, telecommunications data may be more revealing than information obtained through interception of a communication or from stored communications.

It is important to understand that with the proliferation of the Internet of Things and 5G mobile networks, (which are likely to provide far more accurate location data, due to the smaller cells used in such networks), telecommunications data is set to become even more powerful data than it already is today.

Consequently, we suggest that the threshold that applies to the authorisation of disclosure requests for existing data be raised to only apply to serious contraventions (as defined by the TIA Act) which is the threshold for issuing a stored communications warrant.

We again note that the protections or thresholds afforded under the TIA Act may not apply to authorisations of disclosure made pursuant to s280 of the Telco Act.

Scope of the services/communications to which the DR Regime applies

The definition of the relevant services and communications to which Part 5-1A applies is very wide and would, in our view, include communication types that underlie the Internet of Things, i.e. communications between machines, sensors and connected 'things', without the direct involvement of a person. This does not appear meaningful but would, if pursued for implementation, cause exorbitant costs to C/CSPs and imply an explosion in the amount of data that would be required to be retained.

The legislation ought to put beyond doubt that such communications are excluded from the DR Regime.

Conclusion

Communications Alliance looks forward to continued engagement with the PJCIS, the Department of Home Affairs, and other relevant stakeholders on the mutual objective to ensure that Australia has a useful interception and access regime to protect Australians from crime, to enforce law and to enable the intelligence, interception and enforcement agencies to effectively do so in a rapidly evolving digital environment.

As highlighted in our submission, Communications Alliance believes that the current TIA Act and Telco Act would benefit significantly from the elimination of loopholes and a tightening of requirements and limitations to ensure that the DR Regime, while being fit for purpose and effective, does not unnecessarily restrict civil liberties, infringes onto the privacy of individual and creates unintended and unnecessary complexities for Industry.

Attachment A

Entities Seeking Telecommunications Data that are not Authorised under the Assistance and Access Legislation

At **Part 1** is a list compiled by Communications Alliance Carrier Members and submitted to the PJCIS in November 2018, in response to a request from the Committee. It presents a composite picture across the industry of which agencies/departments had, at that time, sought telecommunications data from one or more carriers since the passage of the data retention legislation. The list might not be complete.

At **Part 2** is a list of an additional 27 agencies/departments that have sought telecommunications data from one or more carriers in the period since November 2018. This list might also not be complete.

Please note that:

- a request for metadata does not necessarily mean that the metadata sought was disclosed (in some cases what it sought is not available and/or has not been retained by the time the request is made); and
- in some cases, a single request for metadata results in multiple disclosures, depending on the nature of the request.

Part 1:

Australian Crime Commission
Australian Border Force
ACLEI
AFP
AFP ACT Policing
AFP PROFESSIONAL STANDARDS
AFSA
ASIC
Australian Tax Office
Australia Post Corporate Security Group
Australian Health Practitioner Regulation Agency
BANKSTOWN CITY COUNCIL
BRISBANE CITY COUNCIL
CENTRELINK
CONSUMER & BUSINESS AFFAIRS – VIC
Corrections Intelligence Group – NSW
CRIME AND MISCONDUCT COMMISSION
Customs
Department of Agriculture
Department of Defence
Department of Environment and Conservation WA
DEPARTMENT OF ECONOMIC DEVELOPMENT, JOBS, TRANSPORT & RESOURCES
DEPARTMENT OF IMMIGRATION AND BORDER PROTECTION
DEPT FAIR TRADING NSW
DEPT FAIR TRADING-BRISBANE
DEPT OF COMMERCE WA
DEPT OF FAMILIES, HOUSING COMMUNITY SERVICES
DIBP CANBERRA

DIBP MELBOURNE
DIBP QLD
DIBP SYDNEY
FACS
FAIRFIELD CITY COUNCIL
FAIR WORK BUILDING AND CONSTRUCTION
HEALTHCARE COMPLAINTS COMMISSIONS
IBAC
ICAC SYDNEY
NSW CC
NSW EPA
NSW Office of State Revenue
NSW Police
NSW POLICE PROFESSIONAL STANDARDS
NSW Government Trade, Investment, Resources and Energy
NT POLICE
NTPOL
OFFICE OF ENVIRONMENT & HERITAGE
OFFICE OF STATE REVENUE NSW
Police Integrity Commission – NSW
PRIMARY INDUSTRIES AND RESOURCES SA
PRIMARY INDUSTRIES NSW
PRIMARY INDUSTRIES QLD
PRIMARY INDUSTRIES VIC
QLD Department of Fair Trading
QLD TRANSPORT
Queensland Police Service
Racing Integrity VIC
REGIONAL ILLEGAL DUMPING SQUAD
Rockdale City Council
SA FISHERIES
SA ICAC
SA POLICE ANTI CORRUPTION
SA POLICE INTERNAL INVESTIGATION BRANCH
SA POLICE STATE INTELLIGENCE
TAS POLICE
TAS POLICE INTERNAL INVESTIGATIONS
Taxi Services Commission
TRANSPORT ACCIDENT COMMISSION MELBOURNE
VIC DEPARTMENT OF ECONOMIC DEVELOPMENT, JOBS, TRANSPORT AND RESOURCES
VIC Department of Justice
VIC Department of Health and Human Services
VIC POLICE ETHICAL STANDARDS
VIC INSTITUTE OF TEACHING
VIC POLICE
VIC Sheriff's Offices
WA CCC
WA Department of Fair Trading

WA FISHERIES
WA POLICE STATE INTELLIGENCE DIVISION
Work Safe VIC
WORKPLACE HEALTH & SAFETY

Part 2:
Australian Communications and Media Authority (ACMA)
ASIC WA
Australian Building & Construction Commission
Australian Sports Anti-Doping Authority
Australian Transport Safety Bureau
Clean Energy Regulator
Coroners via NT Police
Coroners via Tas Police
State Coroner's Court
WA Department of Mines, Industry Regulation & Safety
SA Department of Consumer and Business Services
Health Support Queensland
Hunter Region Illegal Dumping Squad
Legal Services Commission
Liverpool City Council
Local Government Investigations and Compliance Inspectorate (Vic.)
National Disability Insurance Agency
NT Office of Information and Public Interest Disclosures
Office of the Health Ombudsman (Qld)
Queensland Office of Industrial Relations
Report Illegal Dumping (NSW)
SafeWork NSW
State Penalties Enforcement Registry (Qld)
Veterinary Surgeons Board of WA
Victorian Building Authority
Victorian Fisheries
Victorian Ombudsman

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507