Additional Remarks from Government Senators

1.1 The government members of the committee acknowledge universal support for reform of the legislative scheme governing telecommunications interception and access.

1.2 Government members agree with the findings of the recent inquiry conducted by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 ('Data Retention Bill'), and support the PJCIS inquiry's recommendation that the Data Retention Bill be passed.[1]

1.3 Government Senators acknowledge the tension that persists between the interests of individual privacy, and national security and note that this tension has been exacerbated by irresponsible public commentary and reporting around the issue of reform of the scheme governing telecommunications interception and access.

1.4 Government members of the committee prefer to view these so-called 'competing' interests—personal/professional privacy, and national security—as inherently complementary interests, and urge a consensus approach to reform.

1.5 The government members of the committee reject the Chair's Report on data access and data retention as an over-simplification of the complex relationship between the complementary interests of national security and individual privacy. The Chair's report examines data retention from a highly biased perspective, and irresponsibly recommends additional layers of tax-payer-funded oversight that duplicate existing protective frameworks and are of limited or no utility.

The Reform Agenda

1.6 The current scheme governing telecommunications interception and access pre-dates mobile telephony and both mobile and fixed data services. It is no longer practicable to rely upon successive amendments to the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to accommodate the pace and breadth of technological change.

1.7 The committee's inquiry revealed a wide range of views regarding the preferable characteristics for reform of the TIA Act. These views overwhelmingly focused on protecting national security, protecting individual rights to privacy, and enhancing administrative efficiencies.

---

1 Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p.xxv.

1.8 Any programme of reform must balance individual interests and national interests with sensitivity, maturity and common sense. The need for balance was clearly expressed by the Australian Law Reform Commission (ALRC) following its 2006-8 review of the *Privacy Act 1988* (Cth):

> As a recognised human right, privacy protection generally should take precedence over a range of other countervailing interests, such as cost and convenience. It is often the case, however, that privacy rights will clash with a range of other individual rights and collective interests, such as freedom of expression and national security. International instruments on human rights and growing international and domestic jurisprudence in this field all recognise that privacy protection is not an absolute.[2]

Streamlining the Warrant Regime

1.9 Compelling evidence was received during the inquiry regarding the complexity of the existing scheme governing warranted access to telecommunications content and metadata. The administrative burden created by intricate process requirements was described *inter alia* by the Director-General of Security:

> Over time, the many amendments to the TIA Act have resulted in duplication and complexity making the Act difficult to understand and apply.[3]

1.10 Government members of the committee support recommendations from law-enforcement and national security agencies calling for the introduction of a single attribute-based warrant scheme for content retrievals and interceptions.[4] Government Senators are persuaded that the targeted nature of attribute-based warrants will lend efficiency and expedience to investigative practices, as well as protecting individual rights to privacy through the observance of proportionality thresholds.

1.11 In supporting the introduction of a single attribute-based warrant scheme ASIO and the ACC noted the need to maintain 'proportionality thresholds and accountability requirements…to deliver public confidence and assurance regarding the use of these powers'.[5] The Law Council of Australia (Law Council) explained:

> …where a State seeks to restrict human rights, such as the right to privacy, for legitimate and defined purposes, for example in the context of telecommunications access and interception, the principles of necessity and proportionality must be applied. The measures taken must be appropriate and the least intrusive to achieve the objective. In the context of

2 *For Your Information – Australian Privacy Law and Practice*, Australian Law Reform Commission (ALRC) Report #108, p. 104.

3 ASIO, *Submission 27*, p. 34.

4 For example ASIO, *Submission 27*, p. 26; Attorney-General's Department (AGD), *Submission 26*, pp. 16-19.

5 ASIO, *Submission 27*, p. 35. See also: ACC, *Submission 23*, p. 14.

> telecommunications access and interception, this involves balancing the intrusiveness of the interference, against operational needs.[6]

1.12 The government members are satisfied that proportionality thresholds are satisfactorily maintained by relevant agencies, through existing procedural and oversight functions, to a standard that may reasonably be anticipated by the community-at-large.

1.13 The government members of the committee are strongly of the view that the utility of a single attribute-based warrant scheme should not be compromised through the imposition of cumbersome and unnecessary limitations or exceptions.

1.14 The protections that are currently conferred upon citizens' in relation to metadata will be substantially improved by the passage of the government's Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

1.15 Government members of the committee acknowledge the privacy implications of changes to warranted access however they are reassured by the government's unambiguous commitment to the preservation of individual privacy within the imperatives of the contemporary risk environment.

Oversight and the Commonwealth Public Interest Monitor

1.16 There is a range of existing oversight mechanisms for access to data and content, including in certain circumstances warrant regimes. These oversight functions protect the public interest in the preservation of individual privacy, as well as the public interest in the protection of national security.

1.17 The government members of the committee are satisfied that existing oversight functions are sufficient and that the introduction of a Commonwealth Public Interest Monitor would unnecessarily duplicate existing processes at the tax-payers' expense. Government members of the committee do not consider that this would reflect the public interest.

Metadata – Definition

1.18 The need for reform to the TIA Act is substantially due to the existing scheme's inability to accommodate the pace and breadth of technological change. The government members of the committee are mindful that inclusion of a prescriptive definition of 'metadata' in the legislative scheme could limit investigative scope in future, thus requiring amendments of the type and frequency that have led to the complexity found in the existing scheme.

---

6 Law Council of Australia, *Submission 34*, p. 5.

1.19 Government members encourage further consultation regarding the technology-neutral definition of all terms across any proposed reform of the TIA Act.

Mandatory Data Retention

1.20 Government Senators fully support the mandatory data retention scheme that is contemplated by the Data Retention Bill that is presently before the Parliament as fundamental to Australia's national security and law enforcement priorities.

1.21 National security and law enforcement agencies have unanimously and unambiguously identified the value derived from telecommunications data in the conduct of investigative activities.[7]

1.22 The Attorney-General's Department has stated that the increasing need for data retention has resulted from technological developments and consequential changes in the business practices of service providers:

> Historically, service providers have generated and retained telecommunications data for their business purposes. However, as providers shift to modern, IP-based networks and services, they are tending to retain a narrower range of data, and to retain that data for shorter periods.[8]

1.23 The government members of the committee acknowledge evidence that mandatory data retention has the potential to provide greater privacy to individuals who may otherwise fall under the gaze of law enforcement investigations where such investigations would be required to cast a wider net in the absence of retained data. For example, the ACC submitted that accessing retained data enabled it to conduct investigations without needing to intercept or access the content of a wider range of communications.[9]

1.24 The ACC noted however that the retention of telecommunications content and data by service providers in Australia is variable and subject to the storage capacity of the service provider in question. The resultant lack of a consistent national standard:

> …results in uncertainty for law enforcement and can jeopardise the outcome of operations. These differences in retention periods create difficulties for the ACC in its ability to undertake investigations into federally relevant criminal activity, as valuable telecommunications data is not always available when needed. When it comes to conducting ACC investigations on long-term federally relevant criminal activity, access to retrospective telecommunications data is critical for the ACC to understand the scope and nature of the threat.[10]

---

7 AGD, *Submission 26*, pp. 3, 4; ASIO, *Submission 27*, pp. 5, 33, 39.

8 AGD, *Submission 26*, p. 30.

9 ACC, *Submission 23*, p. 15.

10 ACC, *Submission 23*, p. 15.

1.25 ASIO explained that it considered that a data retention period of 'at least two years in some cases' is required for it to effectively discharge its functions.[11]

1.26 The Australian Federal Police also supported calls for a mandatory data retention regime, explaining that this would ensure a 'national and systematic approach is taken to safeguarding the ongoing availability of telecommunications data for legitimate purposes'.[12]

Objects Clause

1.27 Government Senators are of the view that the privacy interests of individual citizens are comprehensively protected by a range of existing legislated and regulated oversight functions.

1.28 The protection of individual personal privacy is also implicit in the operation of the TIA Act itself which was enacted to provide a scheme of regulation for the interception of and access to the communications of private individuals. Government Senators are mindful that a prescriptive statement of objectives could have the same limiting effect on this scheme as a prescriptive definition of 'metadata'.

1.29 The inclusion of an objects clause in the TIA Act as an additional clarification of privacy protections would be of limited utility.

Destruction requirement

1.30 Government members of the committee are of the view that service providers are likely to be sufficiently motivated by commercial considerations to purge stored data once any statutory retention period has elapsed and do not believe prescriptive destruction parameters would impact the frequency, immediacy or completeness of the destruction of stored data.

1.31 In addition, the *Privacy Act 1988* (Cth) provides a framework for the destruction of personal information where the information is no longer required under law or for a legitimate business purpose.[13]

Conclusions and Recommendations

1.32 The government members of the committee acknowledge the sensitivity and complexity of debate around the complementary interests of national security and individual rights to privacy. Technological developments such as the proliferation of data mobility have contributed to the intricacies of this debate.

---

11 ASIO, *Submission 27*, p. 27.

12 Australian Federal Police, *Submission 25*, p. 10.

13 *Privacy Act 1988* (Cth), ss 4 and 11.

1.33 Any scheme of reform of the TIA Act must measure the individual interest against the national interest as well as accommodating the interests of commercial operators. The government members of the committee support a considered approach that will focus on consultation in exploring all facets of reform of the TIA Act.

1.34 Government Senators agree with the findings of the PJCIS inquiry into the Data Retention Bill and acknowledge that the government has announced its support for all 39 of the PJCIS report's recommendations. Government members of the committee wholeheartedly support the passage of the Data Retention Bill, and the implementation of a mandatory data retention scheme, as a matter of national urgency.

Recommendation 1

1.35 The government members of the committee recommend the instigation of a single attribute-based warrant scheme to apply to telecommunications content.

Recommendation 2

1.36 The government members of the committee recommend that the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 be passed by the Senate.

Senator the Hon Ian Macdonald
Deputy Chair