1

Introduction

Background to the inquiry

1.1 In May 2012, Attorney-General the Hon. Nicola Roxon MP asked the Parliamentary Joint Committee on Intelligence and Security (the Committee) to inquire into a number of potential reforms to Australia's national security legislation. Subsequent to this request, the Committee was provided with a discussion paper outlining the reforms the Australian Government was considering, as well as some on which the government sought the views of the Committee.

1.2 This discussion paper contained the terms of reference for this inquiry which canvassed reforms in three areas: interception of communications and access to data under the *Telecommunication (Interception and Access) Act 1979*; reform of the telecommunications security aspects of the *Telecommunications Act 1997* and other relevant legislation; and reform of the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*. The terms of reference contained 18 specific reform proposals.

1.3 The Committee formally adopted the proposed terms of reference on 6 July 2012.

1.4 The Committee was faced with two key difficulties in its conduct of this inquiry. Firstly, the terms of reference were very wide-ranging, containing 44 separate items across three different reform agenda. Secondly, the lack of any draft legislation or detail about the potential reforms was a major limitation and made the Committee's consideration of the merit of the reforms difficult. This also made it hard for interested stakeholders to effectively respond to the terms of reference.

Conduct of the inquiry

1.5 The Chair of the Committee, the Hon. Anthony Byrne MP announced the inquiry via media release on 9 July 2012, and the inquiry was subsequently advertised in *The Australian* on 11 July 2012. The Attorney-General's Department discussion paper was published on the Committee website. Letters inviting submissions were sent to over 130 stakeholders in both federal and state government, the telecommunications industry, civil liberties and privacy non-government organisations, and peak legal bodies and associations with an expected interest in the reforms canvassed.

1.6 The Committee received 240 submissions and 29 exhibits. These are outlined in Appendices A and B. Three submissions were received in largely identical terms from some 5,300 individual members of the public. These submitters expressed opposition to the reform proposals, and to a mandatory data retention regime in particular. The Committee thanks these members of the public for contributing to the inquiry and making their concerns known.

1.7 At all times it was the Committee's preference for submission to be made public. Confidentiality was granted by the Committee where the information had a national security classification such as SECRET or where a submitter made a special request for such confidentiality to the Committee.

1.8 Whilst it is the Committee's preference to be open and transparent the use of classified evidence has meant this has not always been possible.

1.9 The Committee is grateful to ASIO and ASIS for providing unclassified submissions. This was particularly helpful in the writing of this report.

1.10 The Committee held six public hearings, three private classified hearings and a further private hearing. The witnesses who appeared at these hearings are outlined in Appendices C and D.

1.11 In addition to its public and classified hearings, the Committee received private briefings from the Attorney-General on two occasions, and received a further private briefing from the Secretary and officials of the Attorney-General's Department.

1.12 As the Committee commenced its inquiry, the Government of the United Kingdom issued a draft Communications Data Bill which has similarities to potential reforms in the Australian Government's proposals. The Bill was examined by the British Intelligence and Security Committee (ISC) and a Joint Select Committee of the UK Parliament. The Committee held a private meeting with the ISC where the reform proposals in each country were canvassed. The

Committee appreciated the observations and assistance provided by ISC members and their Secretariat.

1.13 Finally, the Committee visited Telstra's Global Operations Centre and received useful briefings from Telstra's staff.

1.14 Having commenced the inquiry at the beginning of July 2012, the Committee was asked to report if at all possible by the end of the calendar year. This afforded the Committee a highly compressed and unachievable time frame of less than six months to examine what is an extensive list of potential reforms, some of which are far reaching.

1.15 The Committee thanks all submitters and witnesses, including the large number of members of the public who submitted, for their contributions to the Committee's examination of this package of potential reforms of national security legislation.

1.16 While the evidence submitted was heavily focussed on data retention, the Committee carefully examined each proposal within the Terms of Reference. In its recommendations the Committee has outlined a strategy for the further development of the potential reforms to national security legislation. Specifically, the Committee believes that detailed consideration of any draft legislative provisions will be necessary. Public consultation must be part of this consideration. As part of this consultation the Committee sees merit in expressly seeking the views of key stakeholders including the Independent National Security Legislation Monitor, oversight bodies, privacy advocates, the telecommunications sector, law enforcement and national security agencies.

Structure of the report

1.17 This report focuses around the terms of reference, and thus comprises four chapters. The following chapters discuss:

- Chapter Two – reform of the government's ability to intercept telecommunications content and data via the *Telecommunications (Interception and Access) Act 1979*;
- Chapter Three – reform of telecommunications sector security and relevant legislation such as the *Telecommunications Act 1997*; and
- Chapter Four – reform of the legislation governing the functions and activities of Australia's intelligence community, including the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*.

- Chapter Five – data retention.

1.18 The Terms of Reference group the proposed reforms into three broad categories:

- Matters the Government wishes to progress;
- Matters the Government is considering; and,
- Matters on which the Government expressly seeks the views of the Parliamentary Joint Committee on Intelligence and Security.

1.19 Due to the complexity and number of issues raised in the Terms of Reference it has not always been possible or logical for the Committee to address its comments in accordance with the three broad groupings noted above.

Chapter Two

1.20 Chapter two looks at a series of proposed reforms to the telecommunications interception regime that are designed to better reflect the 'contemporary communications environment'.[1]

1.21 In particular, the AGD identified four aspects of the legislation as requiring reform:

- Strengthening the safeguards and privacy protections in line with contemporary community expectations;
- Reforming the lawful access regime for agencies;
- Streamlining and reducing complexity; and
- Modernising the cost sharing framework.[2]

1.22 Chapter two deals with each of these areas in detail.

Chapter Three

1.23 Chapter three looks at emerging challenges to the security of telecommunications data:

> Risks to the availability, confidentiality and integrity of our national telecommunications infrastructure can come from hardware vulnerabilities, accidental misconfiguration, external hacking and even trusted insiders.[3]

1 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 12.

2 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 22.

3 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 29.

1.24 The implications of these risks are significant, especially given that Australian businesses, individuals and public sector actors rely on telecommunication carriers and carriage service providers' (C/CSPs) ability to store and transmit their data safely and securely, and to protect it from potential national security threats. The discussion paper notes that:

> Failure to effectively manage national security risks therefore has implications beyond individual C/CSPs; it is a negative externality affecting government, business and individual Australians.[4]

1.25 The chapter looks at the proposed package of reforms to the *Telecommunications Act 1997* and associated legislation to establish this regulatory framework.

Chapter Four

1.26 Chapter four deals with a number of practical difficulties with the legislation governing the operation of the Australian Intelligence Community which is comprised of the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Defence Signals Directorate (DSD), and the Defence Imagery and Geospatial Organisation (DIGO), the Defence Intelligence Organisation (DIO) and the Office of National Assessments (ONA).[5]

1.27 In relation to these difficulties, the discussion paper canvasses a number of reforms to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act). According to the discussion paper, these reforms are necessary to:

> ...maintain the intelligence gathering capabilities of the Australian intelligence agencies, ensuring they remain able to adeptly respond to emerging and enduring threats to security. Proposed reforms seek to continue the recent modernisation of security legislation to ensure the intelligence community can continue to meet the demands of government in the most effective manner.[6]

---

4 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 29. An externality refers to a cost or benefit that accrues to actors which are not directly involved in a transaction.

5 On 3 May 2013 the Government announced its intention to rename the DSD and DIGO as the Australian Signals Directorate (ASD) and the Australian Geospatial-Intelligence Organisation (AGO) respectively. <http://www.minister.defence.gov.au/2013/05/03/prime-minister-and-minister-for-defence-joint-media-release-2013-defence-white-paper-renaming-the-defence-signals-directorate-and-the-defence-imagery-and-geospatial-organisation/>, viewed on 6 May 2013.

6 Attorney-General's Department, *Equipping Australia against emerging and evolving threats*, Discussion Paper, July 2012, p. 40.

1.28 Chapter 4 of the report looks into these matters and make recommendations where appropriate.

Chapter Five

1.29 The Government sought the Committee's views on a mandatory data retention regime.[7] The Committee did not have access to draft legislation. Furthermore, the inadequate description of data retention in the terms of reference and discussion paper also impaired both the public discussion and the Committee's consideration of the data retention issue.

1.30 By far the most controversial topic on which the Committee was asked to provide comment, data retention took up much of the Committee's time. The number of submissions on this issue far exceeded those received on any other topic in the terms of reference.

1.31 In correspondence to the Committee, the Attorney-General defined what could potentially be included in a data set for retention. The Attorney-General put forward the European Union data retention directive, which can be found at Appendix F, as an appropriate model.

1.32 Many submitters to this inquiry expressed their concerns about content being retained under any mandatory data retention regime. However, by the conclusion of the evidence gathering phase of the inquiry, the Attorney-General and the AGD had categorically stated that it was not the Government's intention to propose a regime that retains content, such as the substance of text messages and emails. However as Chapter Five reveals, there was conflicting evidence from expert witnesses as to whether this was technically possible. Indeed, one of the issues the Committee confronted was the uncertain definitional boundaries between data and content. For completeness, the definitional issue of what constitutes 'data' and 'content' is included in chapter five.

1.33 The issue with which the Committee has grappled arises not primarily from a changed threat environment, but from the increasingly rapid development of technological capability which has in many cases outpaced the security services' capacity to respond.

1.34 There is no doubt that the enactment of a mandatory data retention regime would be of significant utility to the national security agencies in the performance of their intelligence, counter-terrorism and law enforcement functions. The Committee takes very seriously the security services' concerns for public safety.

7 Attorney-General's Department, *Equipping Australia against emerging and evolving threats,* Discussion Paper, July 2012, p. 40.

1.35 However, a mandatory data retention regime raises fundamental privacy issues, and is arguably a significant extension of the power of the state over the citizen. No such regime should be enacted unless those privacy and civil liberties concerns are sufficiently addressed

1.36 Ultimately, the reconciliation of these two fundamental public values is a decision for Government to make.

1.37 The Committee would have been in a better position to assess the merits of such a scheme, and the public better placed to comment, had draft legislation been provided to it.

Appendices

1.38 In addition to the appendices mentioned above, appendices with relevant information have been provided to assist the reader of the report. They are as follows:

- Appendix E: Discussion paper, *Equipping Australia against emerging and evolving threats*.
- Appendix F: Correspondence from the Attorney-General regarding data retention.
- Appendix G: Correspondence from the Secretary of the Attorney-General's Department further clarifying data retention.
- Appendix H: Telecommunications data provided to law enforcement and national security agencies by Telstra.