Submission No 135

Inquiry into potential reforms of National Security Legislation

Organisation: Ms Irene Graham

Submission

To: Parliamentary Joint Committee on Intelligence and Security

Re: Inquiry into potential reforms of National Security Legislation

From: Irene Graham

Date: 20 August 2012

Table of Contents

---

1. Introduction

1. This submission comments on a relatively small number of proposals, primarily in relation to matters where I have prior knowledge as a result of paying close attention to changes to the interception regime for over a decade and lodging submissions in relation to proposed amendments.

2. Failure to comment on numerous other proposals does not signify lack of concern. To the contrary, I find many of the other proposals extremely worrying. However, the majority of the proposals in the Government Discussion Paper are vague and unclear, making it extremely time consuming to attempt to comment on same. In addition, to the minimal extent that the Discussion Paper offers justification or reason for proposals, the information is inadequate for the purpose of contemplating and commenting on the merits or otherwise of proposals, particularly given in many instances it is far from clear what change, exactly, the government wishes to make, and therefore potential ramifications cannot be considered.

3. I am of the opinion that if the Committee decides to make recommendations in relation to many of the vague proposals, the Committee should recommend to the government that, prior to any amendment Bill/s being tabled in Parliament, an exposure draft of proposed Bill/s should be issued for public comment with a submission period of **three** months, and submissions in response to an exposure draft should be published.

4. I also note that the Terms of Reference state:

> *"The Committee should take account of the interests of the broad range of stakeholders including through a range of public, in camera and classified hearings."*

5. It is a matter of grave concern that the Government terms of reference to a Parliamentary Committee extraordinarily seek to encourage secrecy of hearings. Obviously the Committee is at liberty to decide for itself what, if any, hearings it will conduct in secret. I hope that the Committee will be very cautious about agreeing to take evidence in secret and/or basing any recommendations on secret assertions and information that cannot be subjected to the light of public scrutiny.

2. History of interception regime

6. The Discussion Paper makes the remarkable claim that:

[p.12] "...the interception regime provided by the current Act reflects the use of telecommunications and the structure of the telecommunications industry that existed in 1979 when the Act was made. Many of these assumptions no longer apply, creating significant challenges for agencies in using and maintaining their investigative capabilities under the Act."

7. Being charitable, it appears the authors of the Government Discussion Paper are unaware that since 1994 there have been five major reviews of the interception regime[1], and resultant legislative amendments; most recently the 2005 "Blunn Review"[2] which also had the purpose of updating the interception regime to minimise challenges faced by law enforcement agencies as a result of communications-related technological developments. As stated on the A-G Department web site, the Blunn "*review found that the interception regime had proved remarkably robust in an era of revolutionary technological change. However, it recommended a series of amendments to ensure the ongoing effectiveness of the regime*"[3]. In addition, amendments to the interception regime have been made nearly every year during the last decade at least.

8. I doubt that there have been any relevant *significant* technological developments since 2005, and in my recollection most, probably all, of the 'developments' mentioned in the Discussion Paper existed and were raised in 2005.

3. "Holistic" reform

9. The Discussion Paper asserts:

[p17] "The magnitude of change to the telecommunications environment suggests that further piecemeal amendments to the existing Act will not be sufficient. Rather, holistic reform that reassesses the current assumptions is needed in order to establish a new foundation for the interception regime that reflects contemporary practice."

10. While there may possibly be merit in holistic reform, the contents of the Government Discussion Paper and the time frame for submission to this inquiry are totally unsuitable for a purpose of holistic reform of the highly complex legislative acts that currently exist. Any attempt at holistic review/amendment under such circumstances is vastly more likely than not to result in unintended and highly undesirable consequences.

4. Strengthening the safeguards and privacy protections in line with contemporary community expectations

11. While strengthening safeguards and privacy protections would be very welcome, the overwhelming majority of proposals in the Discussion Paper would result in less privacy protections than currently exists. Hence the intention implied by the "strengthening" proposal does not seem credible.

5. Mandatory data retention

12. The Terms of Reference refer to:

"tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts "

13. However, the Discussion Paper barely mentions the topic of data retention, and fails to offer any justification for such proposal, other than to claim that some service providers have ceased retaining "transactional data", an undefined term.

14. I am generally opposed to data retention due, in part, to the high risks to personal privacy and security inherent in such retention. There are constantly reports of customers' personal information being accidentally disclosed by businesses including telecommunications service providers, and of company databases being accessed by criminals and customer personal information and credit card details etc. being

1 http://www.ag.gov.au/Telecommunicationsinterceptionandsurveillance/Pages/Reviewoftheregulationofaccesstocommunications.aspx

2 Blunn report of the review of the regulation of access to communications - August 2005 http://www.ag.gov.au/Publications/Pages/Blunnreportofthereviewoftheregulationofaccesstocommunications August2005.aspx

3 http://www.ag.gov.au/Telecommunicationsinterceptionandsurveillance/Pages/Reviewoftheregulationofaccesstocommunications.aspx

published. Mandating data retention will increase the potential for, and probability of, unauthorised disclosure and publication of such personal and sensitive information.

15. Furthermore, the suggested two year retention period is unlikely to have any legitimate justification whatsoever. It is improbable that telecommunications service providers have to date been retaining data for longer than is necessary for billing purposes, i.e. probably about two months, because to keep such data for longer than is necessary for the business's purposes would be a breach of the C'th Privacy Act/National Privacy Principles. Hence an explanation for, and detailed justification of, longer retention periods than to date is necessary for the purposes of proper public consideration and debate.

16. Moreover, as stated in the Discussion Paper "*[t]he concept of 'data' is not defined in the TIA Act*". The Government's 2006 decision not to define "data", when amendments were made to introduce stored communications warrants and new rules concerning law enforcement access to "data", was controversial because there are components of telecommunications (e.g. email messages) where it appears arguable whether or not a component is part of the contents or substance of the communication.

17. My recollection is that the 2006 Government considered it too difficult to define "data" for the purposes of regulating law enforcement access. However, if mandatory data retention is to be introduced, it will be essential that "data" and "data sets" be defined in comprehensive and clear detail, and proposed definitions should be made available for public scrutiny and comment.

18. In addition, it is unknown whether the the Government wants data retention to apply to written communications only when they are transmitted via the Internet, or whether all providers of written communication services would be required to retain data, for example, businesses who provide fax transmission services, Australia Post, courier delivery businesses, etc. If not the latter types of communications service providers, why not? What is so special about Internet communications, and/or is it believed that these days criminals use *only* the Internet to communicate?

19. One also wonders whether, if mandatory data retention is implemented, the next wish list item will be requiring all CCTV and road traffic camera providers to retain data / recordings for two years, just in case at some future time a law enforcement agency might want to access an old recording, along with claimed "justification" that other types of data retention had already been mandated.

20. Mandatory data retention treats all citizens as if they are criminals; an utterly inappropriate situation.

6. Establish an offence for failure to assist in the decryption of communications

21. No explanation, let alone justification, has been provided in relation to this Government proposal.

22. Since enactment of the Cybercrime Act 2001, Australian Federal Police have been empowered to obtain a court order requiring a person to decrypt data, whether or not the data is a communication (Section 3LA(2), Crimes Act 1914).

23. In addition, Section 3LA(5) states:

> *(5) A person commits an offence if the person fails to comply with the order. Penalty for contravention of this subsection: Imprisonment for 2 years.*

24. In 2001, the penalty was 6 months, and has been increased at some time or times since then.

25. This provision was highly controversial in 2001 and remains so, for reasons including that a person may have lost their decryption key, or forgotten their password. See, for example, issues and discussion concerning decryption orders in the Report of the Senate Legal and Constitutional Legislation Committee Inquiry into the Provisions of the Cybercrime Bill 2001.

26. I consider that questions should be asked concerning:

(a) how many times since 2001 have police have obtained such a court order. If none, why not.

(b) If such court orders have been obtained and used, what if any problem has been identified with the use of same.

(c) If any problem/s have been identified, how would such problems be resolved by establishing a different offence from the one that already exists.

27. Furthermore, it is my recollection that in 2001 it was expected by the Commonwealth Government that State/Territory Governments would enact similar court order provisions (I may be mistaken, but I think it may have been a topic of discussion within the Model Criminal Code Committee prior to the 2001 Commonwealth Bill).

28. If some or all State/Territory Governments have not enacted similar provisions (in which case presumably they consider such controversial provisions to be inappropriate), that is not a legitimate reason for the Commonwealth to create another or different Commonwealth offence.

7. Proposed standardisation of thresholds for warrant availability/issue

29. The Discussion Paper (p24) appears to make clear that the government wishes to standardise the penalty threshold that enables application for a warrant authorising interception of, and/or access to, communications, although it is unclear whether the government desires to increase or decrease the thresholds.

30. However, I assume the intention is to decrease the 7 year threshold to 3 years, given the majority of proposals are apparently designed to grant the preferences of law enforcement agencies.

31. I am absolutely opposed to any reduction in existing thresholds. If standardisation is to occur, then the penalty threshold must be 7 years or more.

32. Furthermore, according to the Discussion Paper:

> *[p24] "...There are occasions where the general penalty threshold is too high to cover a range of offences for which it is already recognised that general community standards would expect interception to be available. For example, child exploitation offences and offences that can only be effectively investigated by accessing the relevant networks (including offences committed using a computer or involving telecommunications networks) do not meet the general 7 year imprisonment policy threshold."*

33. The example of child exploitation offences appears irrelevant. Under Commonwealth law the max. penalty is 10 years for child exploitation offences comprised of producing, distributing, accessing, possessing with intent to distribute, etc. such material by means of use of a carriage service.

34. Any State or Territory police service is able to choose to investigate/lay charges in relation to suspected/alleged Commonwealth offences. Therefore they have the option of choosing to by-pass limitations, if any, set by their own State/Territory legislature by application for communications interception/access warrants to investigate alleged Commonwealth offences concerning child exploitation material.

35. Moreover, my August 2012 review/check of State/Territory laws reveals that in all States/Territories (except perhaps Tasmania) the max. penalty for distribution, and/or production of child exploitation material is 7 years, and more often 10 years. In relation to offences of possession only, in the majority of State/Territory jurisdictions the max. penalty is 7 or more years (except in Qld (5 years), and SA (5 years for a first offence and 7 years for a subsequent offence) and possibly less than 7 years in Tasmania)[4].

36. If police services in Qld, SA, or Tas, contend that their ability to use Commonwealth offence provisions to obtain interception/access warrants is not good enough for the purpose of investigation of suspected possession offences (i.e. where local law penalty concerning possession only is or may be less than 7 years), then it is, and should continue to be, their problem to convince their State/Territory legislatures to increase penalties such that they would have an option other than using Commonwealth law offence provisions. It would be utterly inappropriate for the Commonwealth to reduce general penalty thresholds for obtaining warrants for a purpose of enabling non-Commonwealth police services to obtain interception/access warrants where relevant State/Territory legislatures are evidently of the opinion that a higher penalty than currently exists in those jurisdictions is not warranted.

8. Reducing the number of agencies able to access communications information

37. The Discussion Paper states:

4 At the time of writing, I have not had time to find the penalty provisions in Tasmanian law because it appears that, unlike in other States/Territories, penalties are not stated in the Criminal Code /Crimes Act.

[p24] "Consideration is also being given to reducing the number of agencies able to access communications information on the basis that only agencies that have a demonstrated need to access that type of information should be eligible to do so."

38. The range of agencies should certainly be reduced, and probably most especially by deleting all, or most, of the civil and pecuniary penalty agencies that acquired power to obtain access to stored communications when the "stored communications" warrants were introduced in 2006 (although such agencies were not and still are not authorised to obtain interception warrants). At that time there was next to no justification provided for the vast range of such agencies that acquired new powers that are, pretty much, akin to enabling them to conduct fishing trips into individuals private stored communications. There absolutely does need to be a competent review conducted into which of such agencies have a clearly demonstrated need to access stored communications and/or telecommunications "data" in specific circumstances, together with consideration of the type of offences and the penalties that apply to any offences in relation to which such agencies claim "a need".

9. Streamlining and reducing complexity in the law

39. Proposals to change rules concerning agency information sharing, record keeping requirements, accountability measures, etc. are extremely concerning.

40. The Discussion Paper asserts numerous problems without explaining what changes are desired to resolve any such problems. Therefore it is impossible to know whether changes would be an improvement or would improperly reduce regulation of agencies activities.

10. Other Proposals

41. As stated in the introduction hereto, many other proposals are of major concern. They are not addressed in this submission due to lack of time, and the inadequacy of the Government Discussion paper for a purpose of facilitating comment.