Advisory Report on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

Parliamentary Joint Committee on Intelligence and Security

December 2018
CANBERRA
© Commonwealth of Australia

ISBN 978-1-74366-943-3 (Printed Version)

ISBN 978-1-74366-944-0 (HTML Version)

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia License.

The details of this licence are available on the Creative Commons website: http://creativecommons.org/licenses/by-nc-nd/3.0/au/.
Contents

Members .............................................................................................................................................. v
Terms of Reference ............................................................................................................................. vii
List of Recommendations ................................................................................................................ ix

The Report

1   The Bill and its referral .............................................................................................................. 1
   Conduct of the inquiry ................................................................................................................... 1
   Committee consideration of timing ............................................................................................ 2

2   Committee comment and recommendations .......................................................................... 3

Appendix A. List of submissions ..................................................................................................... 9
Appendix B. List of public hearings ................................................................................................ 15
Additional comments ..................................................................................................................... 21
Members

Chair
Mr Andrew Hastie MP

Deputy Chair
Hon Anthony Byrne MP

Members
Hon Mark Dreyfus QC, MP  Senator the Hon Eric Abetz Hon
Dr Mike Kelly AM, MP  Senator David Bushby
Mr Julian Leeser MP  Senator Jenny McAllister
Mr Jason Wood MP  Senator Jim Molan AO, DSC
                       Senator the Hon Penny Wong
Terms of Reference

The Attorney-General referred the Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018 to the Committee for inquiry and report.
List of Recommendations

Recommendation 1

2.2 The Committee recommends that the Parliament immediately pass the Telecommunications (Assistance and Access) Bill 2018, following the inclusion of amendments recommended in this report.

Recommendation 2

2.3 The Committee recommends that the industry assistance measures under Schedule 1 of the Telecommunications (Assistance and Access) Bill 2018, so far as they relate to criminal law enforcement, apply to offences with a penalty of a maximum period of three year’s imprisonment or more.

Recommendation 3

2.4 The Committee recommends that State and Territory law enforcement agencies be retained within the scope of the Bill, with the exception of State and Territory independent commissions against corruption which the Committee recommends should be excluded from the scope of Schedule 1 of the Bill.

Recommendation 4

2.5 The Committee recommends that the Bill be amended to incorporate recommendations from the Commonwealth Ombudsman to establish clear authority to inspect and gather information on the exercise of the industry assistance measures by the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission, and State and Territory interception agencies.
This includes express notification requirements and information sharing provisions which would complement the inspection activities of State and Territory oversight bodies.

**Recommendation 5**

2.6 The Committee recommends that the Bill be amended to incorporate suggestions from the Office of the Inspector-General of Intelligence and Security (IGIS) to strengthen oversight of the powers in Schedule 1 of the Bill, as it applies to the Australian Security Intelligence Service (ASIO), the Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD). This includes:

- explicit notification and reporting requirements when issuing, varying, extending or revoking a notice or request under Schedule 1;

- limits on the exercise of Schedule 1 powers (including extending prohibition on systemic weakness to voluntary notices, ensuring decision-makers consider necessity and intrusion on innocent third parties when issuing a notice);

- defences for IGIS officials; and

- clear information sharing provisions.

The IGIS and the Ombudsman should provide assurances directly to the Committee that the amendments agreed to by the Government address their concerns.

**Recommendation 6**

2.7 The Committee recommends that the Bill be amended to provide that Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs) be subject to statutory time limits, and that any extension, renewal or variation of a TAN or TCN also be subject to a statutory time limit.

**Recommendation 7**

2.8 The Committee recommends that the Bill set out a tiered approval system for state and territory initiated Technical Assistance Notices (TANs), under which TANs would be submitted for approval to the Commissioner of the AFP before being issued to the recipient.
The intention of this process of approval would be to ensure consistency in decision making, and reporting, across jurisdictions.

To give effect to this intention, the Commissioner of the AFP must apply the same statutory criteria, and go through the same decision-making process, as would apply if the AFP were the original issuing authority.

Recommendation 8

2.9 The Committee recommends that the Bill be amended to include a requirement that Technical Capability Notices be jointly authorised by the Attorney-General and the Minister for Communications, the latter being able to provide a direct avenue for the concerns of the relevant industry to be considered as part of the approval process.

Recommendation 9

2.10 The Committee notes the evidence of the Director-General of the Australian Signals Directorate that a “systemic weakness” is a weakness that “might actually jeopardise the information of other people as a result of that action being taken”. The Committee also notes the evidence of the Director-General of Security, that the powers in Schedule 1 will not be used to require a designated communications provider to do anything that jeopardises the security of the personal information of innocent Australians. Having regard to those assurances, the Committee recommends that the Bill be amended to clarify the meaning of the term ‘systemic weakness’, and to further clarify that Technical Capability Notices (TCNs) cannot be used to create a systemic weakness.

Recommendation 10

2.11 The Committee recommends that Schedule 1 of the Bill be amended to apply the ‘systemic weakness’ limitation to all ‘listed acts or things’.

The Committee also recommends that the definitions of ‘listed acts or things’ and ‘listed help’ be exhaustive in the Bill.

Recommendation 11

2.12 The Committee recommends that the Bill be amended to allow a designated communications provider, who has been given a capability notice under
subsection 317W(1) of the Bill in relation to a proposed Technical Capability Notice (TCN), to request a binding assessment of:

- whether the proposed technical capability notice would contravene section 317ZG of the Bill;

- the requirements imposed by the notice are reasonable and proportionate;

- compliance with the notice is practicable and technically feasible; and

- the notice is the least intrusive measure that would be effective in achieving the legitimate objective of the notice.

This request would be made in writing to the Attorney-General within a reasonable time limit specified in the consultation notice.

The Committee recommends that two persons be jointly appointed to conduct the assessment:

- One of these persons should have knowledge that would enable them to assess whether proposed TCN would contravene section 317ZG of the Bill, and should be cleared for security purposes to the highest level required by staff members of ASIO, unless the Attorney-General approves a lower security level.

- The second assessor must be a person who has served as a judge in one or more prescribed courts for a period of 5 years; and who no longer holds a commission as a judge of a prescribed court.

- Both persons must agree that:
  - The requirements imposed by the notice are reasonable and proportionate;
  - Compliance with the notice is practicable and technically feasible; and
  - The notice is the least intrusive measure that would be effective in achieving the legitimate objective of the notice.

- The report prepared by the technical expert and the retired judge must also be provided to the Inspector-General of Intelligence and Security.
(for oversight of ASIO) and the Commonwealth Ombudsman (for oversight of the AFP).

**Recommendation 12**

2.13 The Committee recommends that the Government continues to ensure that the IGIS and other Commonwealth oversight bodies have sufficient resources to ensure that they can properly execute their additional responsibilities under the Bill.

**Recommendation 13**

2.14 The Committee recommends that the Bill be amended to allow a provider to request that the Attorney-General approve disclosure of a technical capability. It would be expected that the Attorney-General would agree to such a request except to the extent that doing so would prejudice an investigation or compromise national security. This would complement existing provisions in the Bill that enable a provider to disclose publically the fact that they were issued a technical capability notice.

**Recommendation 14**

2.15 The Committee recommends that the Bill include express provision for a statutory review of the Bill’s operation by the Independent National Security Legislation Monitor, within 18 months of the Bill commencing.

**Recommendation 15**

2.16 The Committee recommends that the Bill include an amendment which puts beyond any doubt suggestions the Bill may impact Parliamentary privilege.

**Recommendation 16**

2.17 The Committee recommends that, once the Bill (as amended) is passed by the Parliament, the Committee:

- commences a review of the new legislation;
- for the purposes of the review, be allowed to hold further public hearings; and
- complete its review of the new legislation by 3 April 2019.
Recommendation 17

2.18 The Committee recommends that the Government:

- Amend clause 317ZG of Schedule 1 to explicitly prohibit an interception agency from asking a designated communications provider to voluntarily implement or build a systemic weakness or vulnerability under a technical assistance request; and

- Amend clause 317ZH of Schedule 1 so that the ‘general limits’ on technical assistance notices and technical capability notices apply equally to technical assistance requests.
1. The Bill and its referral

1.1 On 20 September 2018, the Minister for Home Affairs, the Hon Peter Dutton MP, introduced the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill) into the House of Representatives.

1.2 In his second reading speech, the Minister noted the Bill created a ‘package of reforms that strengthens the ability of Australia’s law enforcement and national security agencies to deal with the challenges of encryption’.

1.3 The Attorney-General, the Hon Christian Porter MP, wrote to the Parliamentary Joint Committee on Intelligence and Security (the Committee) referring the Bill for inquiry and report.

Conduct of the inquiry

1.4 The Committee announced the inquiry by media release on 21 September 2018 and invited submissions from interested members of the public by 12 October 2018.

1.5 The Committee received 105 submissions and 32 supplementary submissions, which are listed at Appendix A.

1.6 The Committee held public hearings on 19 October 2018 and 16, 26, 27 and 30 November 2018, in-camera hearings on 19 October 2018, and private briefings on 26 November 2018.

1.7 On 22 November 2018, the Committee received advice from the Minister for Home Affairs that there was an immediate need to provide agencies with additional powers and to pass the Bill in the last sitting week of 2018. The Minister noted that:
The situation has become more urgent in light of the recent fatal terrorist attack in Melbourne and the subsequent disruption of alleged planning for a mass casualty attack by three individuals …

I am gravely concerned that our agencies cannot rule out the possibility that others may also have been inspired by events in Melbourne to plan and execute attacks … This is particularly concerning as we approach Christmas and the New Year, which we know have been targeted previously by terrorists planning attacks against Australians gathered to enjoy the festive season …

For these reasons I ask that the committee accelerate its consideration of this vital piece of legislation to enable its passage by the parliament before it rises for the Christmas break.¹

**Committee consideration of timing**

1.8 In order to better inform itself of the immediate challenges faced by agencies, the Committee immediately scheduled additional briefings and public hearings with law enforcement and intelligence agencies. These briefings and hearings were held on 26 November 2018. The Committee took evidence from the Australian Security Intelligence Organisation, the Australian Signals Directorate, the Department of Home Affairs, the Australian Federal Police and Victoria Police. The Committee also took evidence from the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman at a public hearing on 27 November 2018.

1.9 The Committee accepts that there is a genuine and immediate need for agencies to have tools to respond to the challenge of encrypted communications. The absence of these tools results in an escalation of risk and has been hampering agency investigations over several years. As the uptake of encrypted messaging applications increases, it is increasingly putting the community at risk from perpetrators of serious crimes who are able to evade detection.

1.10 Responding to these escalating risks, the Committee recommends that the Parliament give urgent consideration to the Bill and its immediate passage.

1.11 The next chapter presents the Committee’s recommendations regarding the Bill.

¹ The Hon Peter Dutton MP, Minister for Home Affairs, *Submission 89*, pp. 1–2.
2. Committee comment and recommendations

2.1 This chapter presents the Committee’s recommendations regarding the Bill.

Recommendation 1

2.2 The Committee recommends that the Parliament immediately pass the Telecommunications (Assistance and Access) Bill 2018, following the inclusion of amendments recommended in this report.

Recommendation 2

2.3 The Committee recommends that the industry assistance measures under Schedule 1 of the Telecommunications (Assistance and Access) Bill 2018, so far as they relate to criminal law enforcement, apply to offences with a penalty of a maximum period of three year’s imprisonment or more.

Recommendation 3

2.4 The Committee recommends that State and Territory law enforcement agencies be retained within the scope of the Bill, with the exception of State and Territory independent commissions against corruption which the Committee recommends should be excluded from the scope of Schedule 1 of the Bill.

Recommendation 4

2.5 The Committee recommends that the Bill be amended to incorporate recommendations from the Commonwealth Ombudsman to establish
clear authority to inspect and gather information on the exercise of the industry assistance measures by the Australian Federal Police (AFP), the Australian Criminal Intelligence Commission, and State and Territory interception agencies.

This includes express notification requirements and information sharing provisions which would complement the inspection activities of State and Territory oversight bodies.

**Recommendation 5**

2.6 The Committee recommends that the Bill be amended to incorporate suggestions from the Office of the Inspector-General of Intelligence and Security (IGIS) to strengthen oversight of the powers in Schedule 1 of the Bill, as it applies to the Australian Security Intelligence Service (ASIO), the Australian Secret Intelligence Service (ASIS) and the Australian Signals Directorate (ASD). This includes:

- explicit notification and reporting requirements when issuing, varying, extending or revoking a notice or request under Schedule 1;

- limits on the exercise of Schedule 1 powers (including extending prohibition on systemic weakness to voluntary notices, ensuring decision-makers consider necessity and intrusion on innocent third parties when issuing a notice);

- defences for IGIS officials; and

- clear information sharing provisions.

The IGIS and the Ombudsman should provide assurances directly to the Committee that the amendments agreed to by the Government address their concerns.

**Recommendation 6**

2.7 The Committee recommends that the Bill be amended to provide that Technical Assistance Notices (TANs) and Technical Capability Notices (TCNs) be subject to statutory time limits, and that any extension, renewal or variation of a TAN or TCN also be subject to a statutory time limit.
Recommendation 7

2.8 The Committee recommends that the Bill set out a tiered approval system for state and territory initiated Technical Assistance Notices (TANs), under which TANs would be submitted for approval to the Commissioner of the AFP before being issued to the recipient.

The intention of this process of approval would be to ensure consistency in decision making, and reporting, across jurisdictions.

To give effect to this intention, the Commissioner of the AFP must apply the same statutory criteria, and go through the same decision-making process, as would apply if the AFP were the original issuing authority.

Recommendation 8

2.9 The Committee recommends that the Bill be amended to include a requirement that Technical Capability Notices be jointly authorised by the Attorney-General and the Minister for Communications, the latter being able to provide a direct avenue for the concerns of the relevant industry to be considered as part of the approval process.

Recommendation 9

2.10 The Committee notes the evidence of the Director-General of the Australian Signals Directorate that a “systemic weakness” is a weakness that “might actually jeopardise the information of other people as a result of that action being taken”. The Committee also notes the evidence of the Director-General of Security, that the powers in Schedule 1 will not be used to require a designated communications provider to do anything that jeopardises the security of the personal information of innocent Australians. Having regard to those assurances, the Committee recommends that the Bill be amended to clarify the meaning of the term ‘systemic weakness’, and to further clarify that Technical Capability Notices (TCNs) cannot be used to create a systemic weakness.

Recommendation 10

2.11 The Committee recommends that Schedule 1 of the Bill be amended to apply the ‘systemic weakness’ limitation to all ‘listed acts or things’.
The Committee also recommends that the definitions of ‘listed acts or things’ and ‘listed help’ be exhaustive in the Bill.

**Recommendation 11**

2.12 The Committee recommends that the Bill be amended to allow a designated communications provider, who has been given a capability notice under subsection 317W(1) of the Bill in relation to a proposed Technical Capability Notice (TCN), to request a binding assessment of:

- whether the proposed technical capability notice would contravene section 317ZG of the Bill;

- the requirements imposed by the notice are reasonable and proportionate;

- compliance with the notice is practicable and technically feasible; and

- the notice is the least intrusive measure that would be effective in achieving the legitimate objective of the notice.

This request would be made in writing to the Attorney-General within a reasonable time limit specified in the consultation notice.

The Committee recommends that two persons be jointly appointed to conduct the assessment:

- One of these persons should have knowledge that would enable them to assess whether proposed TCN would contravene section 317ZG of the Bill, and should be cleared for security purposes to the highest level required by staff members of ASIO, unless the Attorney-General approves a lower security level.

- The second assessor must be a person who has served as a judge in one or more prescribed courts for a period of 5 years; and who no longer holds a commission as a judge of a prescribed court.

- Both persons must agree that:
The requirements imposed by the notice are reasonable and proportionate;

Compliance with the notice is practicable and technically feasible; and

The notice is the least intrusive measure that would be effective in achieving the legitimate objective of the notice.

The report prepared by the technical expert and the retired judge must also be provided to the Inspector-General of Intelligence and Security (for oversight of ASIO) and the Commonwealth Ombudsman (for oversight of the AFP).

Recommendation 12

2.13 The Committee recommends that the Government continues to ensure that the IGIS and other Commonwealth oversight bodies have sufficient resources to ensure that they can properly execute their additional responsibilities under the Bill.

Recommendation 13

2.14 The Committee recommends that the Bill be amended to allow a provider to request that the Attorney-General approve disclosure of a technical capability. It would be expected that the Attorney-General would agree to such a request except to the extent that doing so would prejudice an investigation or compromise national security. This would complement existing provisions in the Bill that enable a provider to disclose publically the fact that they were issued a technical capability notice.

Recommendation 14

2.15 The Committee recommends that the Bill include express provision for a statutory review of the Bill’s operation by the Independent National Security Legislation Monitor, within 18 months of the Bill commencing.

Recommendation 15

2.16 The Committee recommends that the Bill include an amendment which puts beyond any doubt suggestions the Bill may impact Parliamentary privilege.
Recommendation 16

2.17 The Committee recommends that, once the Bill (as amended) is passed by the Parliament, the Committee:

- commences a review of the new legislation;
- for the purposes of the review, be allowed to hold further public hearings; and
- complete its review of the new legislation by 3 April 2019.

Recommendation 17

2.18 The Committee recommends that the Government:

- Amend clause 317ZG of Schedule 1 to explicitly prohibit an interception agency from asking a designated communications provider to voluntarily implement or build a systemic weakness or vulnerability under a technical assistance request; and
- Amend clause 317ZH of Schedule 1 so that the ‘general limits’ on technical assistance notices and technical capability notices apply equally to technical assistance requests.

Mr Andrew Hastie MP
Chair
A. List of submissions

1. ACS
2. Mr Paul Wilkins
   - 2.1 Supplementary to submission 2
   - 2.2 Supplementary to submission 2
   - 2.3 Supplementary to submission 2 (confidential)
3. Ai Group
4. Mr John Reisner
5. Mr Michael Miller
6. Mr Kristofer Eager
7. Vincent Scollo
8. Jack Coughlin
9. Lisa Burgess
10. Ian Platten
11. Ms Tanya Cumpston
12. Name Withheld
13. Kaspersky Lab
14. Name Withheld
15. Mrs Jan Pukallus
16. Dr Vanessa Teague & Dr Chris Culnane
17. Glenn Petrie
18. Department of Home Affairs
18.1 Supplementary to submission 18
18.2 Supplementary to submission 18
18.3 Supplementary to submission 18
18.4 Supplementary to submission 18
18.5 Supplementary to submission 18
18.6 Supplementary to submission 18

19  Celina Truelove
20  Jason Harrop
21  Global Digital Foundation
22  Mr Nicholas Robinson
23  Internet Architecture Board
24  Mr Scott McIntyre
25  Mr Peter Pronczak
26  Mr Craig Marchant
27  Mr Mark Nottingham
28  Joe Zucco
   ▪  28.1 Supplementary to submission 28
29  Coalition of Civil Society Organisations & Technology Companies & Trade Associations
   ▪  29.1 Supplementary to submission 29
30  Dushan Karovic-Wynne
31  FastMail Pty Ltd
32  MIT Internet Policy Research Initiative
   ▪  32.1 Supplementary to submission 32
33  Access Now
   ▪  33.1 Supplementary to submission 33
34  Cybersecurity Coalition
35 Riana Pfefferkorn
   • 35.1 Supplementary to submission 35
   • 35.2 Supplementary to submission 35
36 Police Federation of Australia
37 Information Technology Professionals Association
38 Internet Australia
39 AIIA
40 Australian Information Security Association
41 Optus
42 Cisco
   • 42.1 Supplementary to submission 42
43 Communications Alliance, Ai Group, AIIA & AMTA
44 Telstra
45 Office of the Victorian Information Commissioner
46 Mozilla
47 Australian Human Rights Commission
   • 47.1 Supplementary to submission 47
48 BSA | The Software Alliance
   • 48.1 Supplementary to submission 48
49 Australian Communications Consumer Action Network
50 Mr Eric Wilson
51 Sandra Neal
52 Inspector-General of Intelligence and Security
   • 52.1 Supplementary to submission 52
   • 52.2 Supplementary to submission 52
53 Apple, Inc.
54 Future Wise
55 Civil Society
56 Mr Benjamin Smith
57  Law Enforcement Conduct Commission
58  Mr Nic Bressan
59  Chris Higgins
60  Uniting Church in Australia, Synod of Victoria and Tasmania
   •  60.1 Supplementary to submission 60
61  Mr Daniel Hochstrasser
62  LaunchVic
63  Joint councils for civil liberties
64  Commonwealth Ombudsman
   •  64.1 Supplementary to submission 64
   •  64.2 Supplementary to submission 64
65  Office of the Australian Information Commissioner
66  Dr Zoltan Somogyi
67  MR Jerry Gubecka
68  Name Withheld
69  Name Withheld
70  Name Withheld
71  Name Withheld
   •  71.1 Supplementary to submission 71
   •  71.2 Supplementary to submission 71
72  Name Withheld
73  Name Withheld
74  Name Withheld
75  Independent Commission Against Corruption (New South Wales)
76  Law Council of Australia
   •  76.1 Supplementary to submission 76
77  Mr Mark McDougall
78  Digital Industry Group Inc (DIGI)
   •  78.1 Supplementary to submission 78
LIST OF SUBMISSIONS

79  MEAA
80  Paul Templeton
  ▪  80.1 Supplementary to submission 80
81  Professor Joseph Cannataci, Special Rapporteur on the right to privacy
82  Microsoft Australia (confidential)
83  Confidential
  ▪  83.1 Supplementary to submission 83
84  Confidential
85  Senetas
  ▪  85.1 Supplementary to submission 85
  ▪  85.2 Supplementary to submission 85
86  Corruption and Crime Commission
87  Communications Alliance Ltd
88  Confidential
89  The Hon Peter Dutton MP, Minister for Home Affairs
90  Duane Schouten
91  Iain Macleod
92  Penelope Robards
93  AccessibilityOz
94  Senator the Hon Scott Ryan, President of the Senate
95  Ms Clare O'Neil MP
96  Mr Mark Lane
97  Queensland Police
98  Victoria Police
99  Confidential
100 Confidential
101 Mr Andrew Donnellan
102 Mr David Gates
103  Name Withheld

- 103.1 Supplementary to submission 103

104  Name Withheld

105  Confidential
B. List of public hearings

Friday, 19 October 2018

Committee Room 2R1, Parliament House, Canberra

Department of Home Affairs

- Mr Michael Pezzullo, Secretary
- Mr Hamish Hansford, First Assistant Secretary, National Security and Law Enforcement Policy

Australian Security Intelligence Organisation

- Mr Duncan Lewis, Director-General of Security

Australian Federal Police

- Mr Andrew Colvin, Commissioner

Australian Signals Directorate

- Mr Mike Burgess, Director-General

Australian Criminal Intelligence Commission

- Mr Michael Phelan, Chief Executive Officer

Australian Border Force

- Commissioner Michael Outram, Commissioner

Law Council of Australia

- Mr Arthur Moses, President-elect
- Ms Olga Ganopolsky, Chair, Privacy Law Committee of the Business Law Section
▪ Professor Peter Leonard, Member, Media and Communications Committee
▪ Dr Natasha Molt, Director of Policy, Legal Policy Division

Optus
▪ Mr Andrew Sheridan, Vice President, Regulatory and Public Affairs
▪ Mr Gary Smith, Head of Regulatory Compliance

Telstra
▪ Mr Clive Reeves, Deputy Chief Information Security Officer, AsiaPac
▪ Ms Jane van Beelen, Executive, Compliance and Regulatory Affairs
▪ Mr Ramah Sakul, Principal, Head of Regulatory Compliance

Cisco
▪ Mr Matthew Carling, Security Architect
▪ Mr Eric Wenger, Director, Cybersecurity and Privacy Policy
▪ Mr Tim Fawcett, Director, Government Affairs

Communications Alliance, Ai Group, AIIA & AMTA
▪ Mr John Stanton, Chief Executive Officer
▪ Ms Christiane Gillespie-Jones, Director, Program Management
▪ Mr Patrick Fair, Chair, Communications Security Reference Panel

Australian Industry Group
▪ Mr Tennant Reed, Principal National Adviser, Public Policy
▪ Mr Charles Hoang, Digital Capability and Policy Lead

Australian Information Industry Association
▪ Ms Kishwar Rahman, General Manager, Policy and Advocacy

Microsoft (in-camera)
▪ Mr Norman Barbosa, Assistant General Counsel, Law Enforcement and National Security
▪ Mr David Masters, Corporate Affairs Director, Microsoft Australia

BSA | The Software Alliance
▪ Mr Darryn Lim, Director, Policy, APAC
LIST OF PUBLIC HEARINGS

Electronic Frontiers Australia

- Mr Angus Murray, Chair, Policy Committee

Blueprint for Free Speech

- Dr Suelette Dreyfus, Executive Director

Future Wise

- Mr Justin Clacherty, Leadership Team

Friday, 16 November 2018

Sydney Masonic Conference and Function Centre, 66 Goulburn Street, Sydney

Massachusetts Institute of Technology

- Mr Daniel J. Weitzner, Founding Director – MIT Internet Policy Research Initiative

Individuals appearing in their private capacity

- Ms Riana Pfefferkorn
- Dr Vanessa Teague
- Dr Chris Culnane

Inspector-General of Intelligence and Security

- The Hon Margaret Stone, Inspector-General
- Mr Jake Blight, Deputy Inspector-General
- Ms Christina Raymond

Commonwealth Ombudsman

- Mr Michael Manthorpe, Commonwealth Ombudsman
- Ms Jaala Hinchcliffe, Deputy Ombudsman
- Ms Emma Cotterill, Director, National Assurance and Audit
- Mr James Turner, Acting Assistant Director, National Assurance and Audit

Australian Human Rights Commission

- Mr Edward Santow, Human Rights Commissioner
- Mr John Howell, Director, Human Rights and Scrutiny
- Ms Jennifer Lim, Senior Lawyer
- Ms Ella Kucharova, Senior Lawyer
Communications Alliance

- Mr John Stanton, Chief Executive Officer
- Ms Christiane Gillespie-Jones, Director, Program Management

Internet Australia

- Dr Paul Brooks, Chairman
- Ms Holly Raiche, Director

Internet Architecture Board

- Mr Martin Thomson, Member

Monday, 26 November 2018

Parliament House, Canberra

Australian Security Intelligence Organisation

- Mr Duncan Lewis, Director-General of Security
- Ms Heather Cook, Deputy Director-General

Australian Federal Police

- Commissioner Andrew Colvin
- Ms Leanne Close, Deputy Commissioner National Security
- Mr Neil Gaughan, Deputy Commissioner Operations

Australian Signals Directorate

- Mr Mike Burgess, Director-General

Department of Home Affairs

- Mr Mike Pezzullo, Secretary
- Mr Marc Ablong, Deputy Secretary Policy Group
- Mr Andrew Warnes, Assistant Secretary, National Security Policy

Tuesday, 27 November 2018

Parliament House, Canberra

Inspector-General of Intelligence and Security

- The Hon Margaret Stone, Inspector-General
- Mr Jake Blight, Deputy Inspector-General
- Ms Christina Raymond
Commonwealth Ombudsman

- Ms Jaala Hinchcliffe, Acting Commonwealth Ombudsman

UN Special Rapporteur on the right to privacy

- Professor Joseph Cannataci, United Nations Special Rapporteur on the right to privacy
- Dr Elizabeth Coombs, Advisor SRP Team, University of Malta

Friday, 30 November 2018

Parliament House, Canberra

Senetas

- Mr Francis Galbally, Chairman
- Mr Andrew Wilson, Chief Executive Officer

Consilium International Group

- Mr Michael Zarew, Chief Executive Officer

Access Now

- Mr Nathaniel White, Senior Legislative Manager

Digital Rights Watch

- Ms Elizabeth O’Shea, Board Member
Additional comments

The fundamental responsibility of any government is to ensure the safety of the nation and its people. It is the foundation upon which all other policy aspirations necessarily rest. As a party of government, it is a responsibility that Labor has always upheld.

Meeting this responsibility requires coordinated action by parliament and the executive. This has never been more true than over the past two decades, when Australia has faced a diverse range of serious and evolving threats.

During this time the parliament has considered a number of bills that increased the powers and capabilities of our security agencies. With a few limited exceptions, these bills responded to advice from the agencies about the tools they need to keep Australians safe. Labor has always taken the advice from the security agencies seriously. In line with this, the parliament has passed security legislation in an appropriately considered and expeditious way.

The Parliamentary Joint Committee on Intelligence and Security is not a brake on this process – it is an essential part of it.

Government’s ability to respond to new and evolving threats relies on the public’s ongoing faith that our national security laws are appropriate, proportional, and adapted to the circumstances we face.

The committee’s work builds that faith. The public process of authorising and reauthorising laws that the committee undertakes is an essential exercise in democratic accountability. It is an acknowledgment of the potential for new
powers to impinge on the fundamental rights and values of Australians. It is also an opportunity to ensure that the resources and powers provided to agencies are as effective as is possible given the nature of the threat environment.

The committee has undertaken this work in a deliberate, sensible, and bipartisan way through changing circumstances, governments, and prime ministers for decades.

The work of the committee has not been assisted by the government’s approach to this debate over recent weeks. Labor members are concerned to avoid a continuation of this conduct. It jeopardises the important function the committee serves in our national security apparatus.

The substance of the Bill

Labor members would like to thank the acting Minister for Home Affairs for the cooperative and constructive approach he has taken to discussions.

We are pleased that the government has acknowledged and responded to a number of the serious concerns raised both by Labor members of the committee, and by the opposition more broadly.

Labor members welcome the amendments that have been proposed in the committee’s report, including:

- enhancing the oversight provisions;
- narrowing the range of offences to which the bill applied;
- defining key terms relating to systemic weaknesses and vulnerabilities; and
- adopting enhanced scrutiny and authorisation processes.

These amendments make the Bill better – and make Australians safer.

However, we do not consider that these amendments address all of the problems in this Bill.

Labor members have moved to progress this Bill despite our concerns because of the evidence from law enforcement and security agencies that there is a need for these powers over the Christmas period, and because the proposed amendments deliver adequate oversight and safeguards to prevent unintended consequences while ongoing work continues.

We are only prepared to take this course of action because of the government’s undertaking that:

- the committee will continue its inquiry into the Bill into 2019, and
• a separate statutory review will be undertaken by the Independent National Security Legislation Monitor within 18 months of the legislation coming into effect.

These separate processes provide an opportunity to resolve our ongoing concerns about the Bill with the assistance of industry, experts, and civil liberties groups, whilst also upholding our responsibility to keep Australians safe.

This compromise is emblematic of the balancing exercise that the committee has undertaken in all its work over the decades. The government should not walk away from it again.

The Hon Anthony Byrne MP
Deputy Chair

The Hon Mark Dreyfus QC MP

The Hon Dr Mike Kelly AM, MP

Senator Jenny McAllister
Senator the Hon Penny Wong