UNSW AUSTRALIA
Canberra
Never Stand Still

Australian Centre for Cyber Security

School of Engineering and IT

Committee Secretary

Parliamentary Joint Committee on Intelligence and Security

PO Box 6021

Parliament House

Canberra ACT 2600

3 February 2017

Submission: Review of the Telecommunications and Other Legislation Amendment Bill 2016

Introduction.

We thank the PJCIS for the opportunity to make this submission.

The submission is made as part of the research conducted by the Australian Centre for Cyber Security (ACCS), in association with UNSW Law. The ACCS is located within the School of Engineering (SEIT) at the Australian Defence Force Academy (ADFA).

The ACCS "…brings together the biggest concentration of research and tertiary education for the multi-disciplinary study of cyber security in any single university in the Southern hemisphere. A number of ACCS scholars, in areas ranging from information technology and engineering to law and politics, have significant international reputations for their work. ACCS serves as a national hub for policy related research and education across the

full spectrum of cyber security (hardware, software, payload, networks, policy, human factors, organizational factors and the information ecosystem)."[1]

Two key issues.

The Telecommunications and Other Legislation Amendment Bill 2016 (the Bill) proposes two key issues that we would like to address:

1. The Bill requires Telecommunications Companies (the TelCo) to do its best to protect telecommunications infrastructure, in the national interest. In this regard, the TelCo is also required to exercise competent supervision over the telecommunications network.[2]
2. The Bill grants the Office of the Attorney-General (AGD), specifically the Attorney General's Secretary (AGS), the power to collect any type of information from the TelCo:
    a. This power is only overseen in terms of an annual report submitted by the AGD to Parliament.
    b. This power may be delegated to the Director-General of the ASIO.
    c. The ASIO may in turn share the information gathered with the AFP and third parties.[3]

Doing-Your-Best and Exercising Competent Supervision over the Network.

In an effort to do its best and exercising competent supervision, the TelCo may adopt a cyber security strategy based on 'situational awareness' and 'threat intelligence'.[4] Situational awareness and threat intelligence may mean the TelCo must have greater visibility of most of the metadata generated by various devices connected to its network. The TelCo must also be aware of the habits of the individual users of the devices. In doing so the TelCo may deploy Deep Packet Inspection (DPI). This may give the TelCo greater contextual awareness of the metadata and relate that to user habits and behaviour, in an effort to identify bad traffic. Using metadata to detect and resolve cyber security threats quicker and in near real-time is a developing trend. The TelCo may

[1] https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/
[2] Telecommunications and Other Legislation Amendment Bill 2016 (Cth).
[3] Ibid.
[4] Qosmos. (2015). DPI and Metadata for Cybersecurity Applications. Retrieved from http://www.qosmos.com/wp-content/uploads/2015/08/Qosmos_DPI_and_Metadata-Cybersecurity_Applications.pdf; Shackleford, D. (2015). Who's Using Cyberthreat Intelligence and How? Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767; Verizon. (2016). Verizon 2016 Data Breach Investigations Report. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

therefore retain more metadata, and for longer, than it usually would.[5] Not retaining and not analysing session metadata may not qualify as doing your best and exercising competent supervision, if that is what the law would require.

Session Metadata as 'any information'.

The metadata includes IP (Internet Protocol) source and destination addresses; source and destination port addresses; and protocol numbers. It therefore includes URLs / web browsing history. This submission specifically focusses on this 5-tuple. This is the session metadata. The 5-tuple falls within the pool of 'any information' the AGS and ASIO may collect from the TelCo.[6]

This metadata may need to be collected from most devices connected to the Internet, and may be stored. The relevant services from which the metadata is harvested includes Web Apps, which are OTT content and communication services, which in turn are excluded from the Metadata Creation, Retention and Disclosure Regime. However, under the TSSR, the TelCo is indirectly made responsible to detect and prevent known and emergent cyber threats, incidents and attacks that may result from the use of OTT content and communication services.[7] Web Apps are heavily targeted by cyber threats and attacks.[8] Under the Metadata Creation, Retention and Disclosure Regime, the TelCo is however not required to use DPI to inspect the packets of Web Apps provided by third

[5] Qosmos. (2015). DPI and Metadata for Cybersecurity Applications. Retrieved from http://www.qosmos.com/wp-content/uploads/2015/08/Qosmos_DPI_and_Metadata-Cybersecurity_Applications.pdf; Shackleford, D. (2015). Who's Using Cyberthreat Intelligence and How? Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767; Verizon. (2016). Verizon 2016 Data Breach Investigations Report. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf; Webb, J., Maynard, S., Ahmad, A., & Shanks, G. (2014). Information Security Risk Management: An Intelligence-Driven Approach. 2014, 18(3). doi:10.3127/ajis.v18i3.1096; Gouglidis, A., Green, B., Busby, J., Rouncefield, M., Hutchison, D., & Schauer, S. (2016, 13-15 Sept. 2016). Threat awareness for critical infrastructures resilience. Paper presented at the 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM).

[6] Ibid; Cisco. (2011). IP Addressing: NAT Configuration Guide, Cisco IOS Release 12.4T (December 18, 2011 ed.). San Jose, CA

[7] Optus. (2015). Submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (pp. 1-21). Australia: Optus; Patton, L. (2016). Telecommunications Sector Security Reforms (pp. 1-3); Group), A. I. G. A., (AIIA), A. I. I. A., (AMTA), A. M. T. A., & Alliance, C. (2016). Submission to the Attorney-General's Department on the Second Exposure Draft of the Telecommunications and Other Legislation Amendment Bill 2015; TPG. (2016). Submission to the Attorney-General's Department on the exposure draft Telecommunications and Other Legislation Amendment Bill 2015 (pp. 104); Group), A. I. G. A., (AIIA), A. I. I. A., (AMTA), A. M. T. A., & Alliance, C. (2016). Submission to the Attorney-General's Department on the Second Exposure Draft of the Telecommunications and Other Legislation Amendment Bill 2015.

[8] Shackleford, D. (2015). Who's Using Cyberthreat Intelligence and How? Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767; Verizon. (2016). Verizon 2016 Data Breach Investigations Report. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

parties, accessed via an Internet access service provided by the TelCo.[9] On the other hand, if the TelCo provides its own OTT content and communications service, such as VoIP, the TelCo is required to create, retain and disclose session metadata, i.e. the 5-tuple. This may require the use of DPI.

Collecting and Sharing Session Metadata as 'any information'.

There are no clear public guidelines and oversight mechanisms regarding the collection and sharing of the 5-tuple information between the AGS, ASIO, the AFP and third parties. The metadata under the TSSR is more information than what is addressed under the Metadata Creation, Retention and Disclosure Regime. However, under the Metadata Creation, Retention and Disclosure Regime new oversight powers have been introduced. This may lead to forum-shopping by the agencies, between the TSSR and the Metadata Creation, Retention and Disclosure regimes.

The two regimes both address the key issue of national security and therefore effectively duplicate the metadata creation, retention and disclosure obligations of the TelCo. Specifically, access to the same metadata by both regimes is a duplication, except that the Metadata Creation, Retention and Disclosure Regime leaves a gap regarding the 3-tuple. The 3-tuple is the destination IP, destination port and protocol number. The gap is that is that the 3-tuple is not required to be retained and is not being disclosed by the TelCo to the agencies. The 3-tuple may potentially be required to be disclosed to the AGS and the agencies under the TSSR, in terms of the Bill.

Both regimes essentially address the same metadata but with different procedures. These differences may result in oversight, governance and ethical risks. No clear boundaries are made as to how overlaps are to be addressed between collecting the information for the purposes of national security under the TSSR, and for the purpose of law enforcement under the Metadata Creation, Retention and Disclosure Regime.

[9] Department, A. G. s. (2015). Data Retention Frequently Asked Questions for Industry. Canberra: Attorney General Department Retrieved from <https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/DataRetentionIndustryFAQS.pdf>.

Links between the TSSR and the Metadata Creation, Retention and Disclosure regimes.

Under the Metadata Creation, Retention and Disclosure Regime, the TelCo is not required to retain the 3-tuple. The TelCo may voluntarily retain this metadata. In doing its best to protect the telecommunications infrastructure and exercise competent supervision, the TelCo may be necessitated to adopt a strategy to actually retain this metadata and for longer[10], as stated above. In other words, under the TSSR, the TelCo may be indirectly required to retain destination IP and destination port addresses and protocol numbers. This may result in the retention of the 5-tuple. It makes little sense not to simultaneously retain destination information under a 'situational awareness' and 'threat intelligence' strategy. The source and destination metadata require to be matched and analysed to identify emergent threats, incidents and attacks.[11]

The TelCo is also not specifically required to disclose the 3-tuple to the agencies as 'retained data', because this information is not clearly categorised as metadata. The 3-tuple is neither clearly classified as content, that requires a warrant to access and use.[12] It is therefore not clear whether a warrant may be required for the agencies to access and use this information.

Within this unclear environment, the AGS may be empowered to collect any information from the TelCo. Additionally, the Director-General of the ASIO may collect the same information, and share it with the AFP and third parties, with no clear public guidelines regarding its access and use.

Under the policy position of the AGD regarding the Metadata Creation, Retention and Disclosure Scheme, the TelCo is not required to use DPI to retain metadata.[13] The TelCo

[10] Qosmos. (2015). DPI and Metadata for Cybersecurity Applications. Retrieved from http://www.qosmos.com/wp-content/uploads/2015/08/Qosmos_DPI_and_Metadata-Cybersecurity_Applications.pdf; Shackleford, D. (2015). Who's Using Cyberthreat Intelligence and How? Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767

[11] Ibid; TPG. (2016). Submission to the Attorney-General's Department on the exposure draft Telecommunications and Other Legislation Amendment Bill 2015 (pp. 104);

[12] Telecommunications (Interception and Access) Act (No 114) 1979 (Cth); Explanatory Memorandum, Telecommunications (Interception And Access) Amendment (Data Retention) Bill 2015 (No 44) (Cth). Canberra: THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA Retrieved from <http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c/upload_pdf/501754%20Revised%20EM.pdf;fileType=application%2Fpdf#search=%22legislation/ems/r5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c%22>.

[13] Department, A. G. s. (2015). Data Retention Frequently Asked Questions for Industry. Canberra: Attorney General Department Retrieved from <https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/DataRetentionIndustryFAQS.pdf>.

is informed by policy of the AGD not to retain metadata if it does not have the visibility of the information or does not have it available.[14] This, despite the legal duty to create the metadata the TelCo is required to retain.[15] These policy exceptions may be best if provided for by means of statutory instruments instead. However, the TelCo would be required to do its best, exercise competent supervision, prevent interference and unauthorised access to information and communications under the TSSR. This may require the use of DPI and harvesting of metadata. These are potentially conflicting positions between the law and policy and the two regimes. It may require harmonisation if the TelCo is required to comply with the laws and is at risk of being penalised for non-compliance.

Conclusions.

Overall, the metadata under both regimes are just the same metadata at the end of the day. The same metadata is accessed for the same purposes: law enforcement and national security. However, the oversight mechanisms regarding access for security under the two regimes differ vastly. The purpose for this difference in treatment is not made clear. Metadata under the TSSR, which is the vast majority of session metadata and may have greater privacy implications, require no authorisation and notification process, and little independent oversight, unlike the source IP and port addresses under the Metadata Creation, Retention and Disclosure Regime.

The Commonwealth Ombudsman is not granted oversight powers over the AFP over TSSR metadata unlike with metadata collected under the Metadata Creation, Retention and Disclosure Regime. It may therefore be worthwhile to align the TSSR and the Metadata Creation, Retention and Disclosure regimes so as to avoid fragmentation in terms of data types, retention requirements, disclosure rules and oversight.

[14] Department, A. G. s. (2015). Data Retention Frequently Asked Questions for Industry. Canberra: Attorney General Department Retrieved from <https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/DataRetentionIndustryFAQS.pdf>.

[15] Telecommunications (Interception and Access) Act (No 114) 1979 (Cth); Explanatory Memorandum, Telecommunications (Interception And Access) Amendment (Data Retention) Bill 2015 (No 44) (Cth). Canberra: THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA Retrieved from <http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c/upload_pdf/501754%20Revised%20EM.pdf;fileType=application%2Fpdf#search=%22legislation/ems/r5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c%22>.

Recommendations.

1. The TSSR and Metadata Creation, Retention and Disclosure Regime may need to synchronize its policy measures regarding DPI and OTT content and communications services provided by third parties.
2. Clarify the legal and policy ambiguities regarding the types of metadata and oversight under the two regimes.
3. Introduce public rules for sharing metadata between AGD, ASIO, AFP and third parties.
4. Introduce rules regarding overlap and scope, between law enforcement and national security investigations.
5. Prevent bypassing of the Metadata Creation, Retention and Disclosure Regime due to duplication by the TSSR.
6. Introduce an Authorisation and Notification Regime under TSSR.
7. Prevent forum-shopping by the agencies.
8. Specify oversight by Commonwealth Ombudsman and IGIS under TSSR.
9. Classify URLs/web browsing history as content that requires a warrant to access.

Further information.

For further information please view this presentation on the subject: https://www.youtube.com/watch?v=PKKABwRacUI /

The PowerPoint presentation referred to in the talk can be found here: https://www.cryptoparty.in/sydney#section2017 / https://ln.sync.com/dl/fb8324dc0#bs2uyv3t-6uddyfvi-wusebzak-f95bfnkv

The key authors of the submission are:

Stanley Shanapinda — Ph.D. Candidate

Dr. Alana Maurushat — Senior Lecturer: UNSW Law

We thank you for the opportunity to make the submission.

Professor Jill Slay AM

PhD, FACS, CP, MIEEE, Fellow of (ISC)2, CISSP, CCFP

Director Australian Centre for Cyber Security, School of Engineering and Information Technology

www.accs.unsw.adfa.edu.au

ADFA
AUSTRALIAN DEFENCE FORCE ACADEMY

Dislcosure: The researchers, Dr. Alana Maurushat and Ph.D. Candidate Stanley Shanapinda are also associated with the Data to Decisions CRC (D2D CRC) (http://www.d2dcrc.com.au/).

References:

ACMA. (2015). *Communications report 2014–15*. Retrieved from Canberra: <http://www.acma.gov.au/~/media/Research%20and%20Analysis/Report/pdf/ACMA%20Communications%20report%202014-15%20pdf.pdf>

AFP. (2016). *Freedom of information request*. Australia: Commonwealth of Australia Retrieved from <https://www.righttoknow.org.au/request/1498/response/5643/attach/2/Decision%20letter%20and%20documents%202016%20324%20reduced.pdf>.

ASIO. (2015). *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014: Supplementary Information*. Australia: Commonwealth of Australia Retrieved from http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Submissions.

Australia, C. o. (2016). *Australia's Cyber security Strategy*. Retrieved from https://cybersecuritystrategy.dpmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf?q=270716.

Australian Security Intelligence Organisation Act (Cth), Federal Register of Legislation § 8A, 16, 18,19, 19A, 113 Stat. (1979 25 October 1979).

BILLS Telecommunications and Other Legislation Amendment Bill 2016 Second Reading SPEECH. (2016). In Senate (Ed.).

CAC, C. A. C. (2015). *Data Retention Implementation Plan and/or Exemption and/or Variation Application*. Canberra: Attorney-General, Office of the Retrieved from https://www.tio.com.au/__data/assets/word_doc/0006/188754/Data-Retention-Application-Template-v1.0-May-2015.DOCX.

Centre, A. C. S. (2016a). *ACSC Threat Report 2016*. Retrieved from https://www.google.com.au/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiahLSMzrLRAhUFtpQKHczUDJ8QFggZMAA&url=https%3A%2F%2Fwww.acsc.gov.au%2Fpublications%2FACSC_Threat_Report_2016.pdf&usg=AFQjCNHrTHSHFZgGYuUW1MQ3tGToUGZU4Q&bvm=bv.142059868,d.dGo

Centre, A. C. S. (2016b). *Australian Cyber Security Centre Threat Report 2016*. Retrieved from https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf.

Cisco. (2011). *IP Addressing: NAT Configuration Guide, Cisco IOS Release 12.4T* (December 18, 2011 ed.). San Jose, CA: Cisco.

Corones, S., & Lane, B. (2010). *Deakin Law Review, 15*(1), 1-36.

Department, A. G. s. (2015). *Data Retention Frequently Asked Questions for Industry*. Canberra: Attorney General Department Retrieved from <https://www.ag.gov.au/NationalSecurity/DataRetention/Documents/DataRetentionIndustryFAQS.pdf>.

Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 29 January 2015

Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 30 January 2015 House of Representatives. 1-85.

Explanatory Memorandum Telecommunications and Other Legislation Amendment Bill 2016 (Cth). (2016).

Explanatory Memorandum, Telecommunications (Interception And Access) Amendment (Data Retention) Bill 2015 (No 44) (Cth). Canberra: THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA Retrieved from <http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_ac4732e1-

5116-4d8f-8de5-0ead3828012c/upload_pdf/501754%20Revised%20EM.pdf;fileType=application%2Fpdf#search=%22legislation/ems/r5375_ems_ac4732e1-5116-4d8f-8de5-0ead3828012c%22>.

Gouglidis, A., Green, B., Busby, J., Rouncefield, M., Hutchison, D., & Schauer, S. (2016, 13-15 Sept. 2016). *Threat awareness for critical infrastructures resilience.* Paper presented at the 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM).

Government, A. (2015). *Telecommunications Sector Security Guidelines*. Retrieved from https://www.ag.gov.au/Consultations/Documents/Telecommunications-Sector-Security-Reforms/Telecommunications-Sector-Security-Guidelines-Draft-Guidelines.pdf.

Group), A. I. G. A., (AIIA), A. I. I. A., (AMTA), A. M. T. A., & Alliance, C. (2016). *Submission to the Attorney-General's Department on the Second Exposure Draft of the Telecommunications and Other Legislation Amendment Bill 2015*

(Telecommunications Sector Security Reform) January 2016. Retrieved from https://www.ag.gov.au/NationalSecurity/Documents/Submission-November-2015-AIG-AIIA-AMTA-CA.pdf

Herrick, D. (2016). *The Social Side of 'Cyber Power'? Social Media and Cyber Operations*. Paper presented at the Proceedings of the 8th International Conference on Cyber Conflict. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2803669

Huston, G. (2015). Metadata Retention and the Internet. *Australian Journal of Telecommunications and the Digital Economy, 3*(1). doi:http://dx.doi.org/10.18080/ajtde.v3n1.4

Hutchinson, V. (2016). Submission to the Attorney-General's Department on the exposure draft Telecommunications and Other Legislation Amendment Bill 2015 (pp. 1-5).

Kokkonen, T. (2016). Architecture for the Cyber Security Situational Awareness System. In O. Galinina, S. Balandin, & Y. Koucheryavy (Eds.), *Internet of Things, Smart Spaces, and Next Generation Networks and Systems: 16th International Conference, NEW2AN 2016, and 9th Conference, ruSMART 2016, St. Petersburg, Russia, September 26-28, 2016, Proceedings* (pp. 294-302). Cham: Springer International Publishing.

Lawrence, J. (2015). Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (pp. 1-27). Australia: Electronic Frontiers Australia.

Optus. (2015). Submission to the Parliamentary Joint Committee on Intelligence and Security *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (pp. 1-21). Australia: Optus.

Patton, L. (2016). Telecommunications Sector Security Reforms (pp. 1-3).

Patton, L. (2017). Internet Australia seeks data retention rethink [Press release]. Retrieved from https://www.internet.org.au/docs/media/477-5-january-2017-news-release-internet-australia-seeks-data-retention-rethink-and-wants-new-parliamentary-inquiry/file

Qosmos. (2015). *DPI and Metadata for Cybersecurity Applications*. Retrieved from http://www.qosmos.com/wp-content/uploads/2015/08/Qosmos_DPI_and_Metadata-Cybersecurity_Applications.pdf

Security, I.-G. o. I. a. (2015). *Annual Report 2014–2015*. Retrieved from Canberra: https://www.igis.gov.au/sites/default/files/files/Annual-Reports/2015/IGIS_AR_14-15.pdf

Security, P. J. C. o. I. a. (2013). *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. Canberra: Commonwealth of Australia Retrieved from

Shackleford, D. (2015). *Who's Using Cyberthreat Intelligence and How?* Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767

Shanapinda, S. (2017). Retention and disclosure of location information and location identifiers *Australian Journal of Telecommunications and the Digital Economy, 4*(4), 251-279. doi:http://dx.doi.org/10.18080/ajtde.v4n4.68

Society, T. I. (2006). SDP: Session Description Protocol (pp. 49): IETF.

Telecommunications (Interception and Access) Act (No 114) 1979 (Cth).

Telecommunications Act (No 47) 1997 (Cth), § 7, 276, 280, 291A, 313, 47 Stat. 10 (Commonwealth of Australia 22 April 1997).

Telecommunications and Other Legislation Amendment Bill 2016 (Cth).

TPG. (2016). Submission to the Attorney-General's Department on the exposure draft Telecommunications and Other Legislation Amendment Bill 2015 (pp. 104).

Verizon. (2016). *Verizon 2016 Data Breach Investigations Report*. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Webb, J., Maynard, S., Ahmad, A., & Shanks, G. (2014). Information Security Risk Management: An Intelligence-Driven Approach. *2014, 18*(3). doi:10.3127/ajis.v18i3.1096