LA TROBE UNIVERSITY

Submission by the

La Trobe University Optus Cybersecurity Research Hub

to the

Parliamentary Joint Committee on Intelligence and Security (PJCIS)

REVIEW OF THE MANDATORY DATA RETENTION REGIME

1 July 2019

Submission Title:

Young Australians a.k.a., 'Digital Natives', Who are Tech-Savvy, Environmentally-Woke and Politically Savvy; and Whistle-blowers; are Potentially Most at Risk of Being 'Spied' On Under Australia's Unique Location Data Retention and Disclosure Scheme - in the Name of 'Security'.

To: Committee Secretary
PO Box 6021
Parliament House
Canberra ACT 2600
Phone: +61 2 6277 2360
Fax: +61 2 6277 2067
pjcis@aph.gov.au

ENQUIRIES
Dr. Stanley Shanapinda
Research Fellow
La Trobe University
Victoria 3086

T 03 9479 3721
E s.shanapinda@latrobe.edu.au
latrobe.edu.au

Table of contents

1.	**INTRODUCTION**	**3**
2.	ABOUT THE LA TROBE UNIVERSITY OPTUS CYBERSECURITY RESEARCH HUB	**4**
3.	EXECUTIVE SUMMARY	**4**
4.	THE TERMS OF REFERENCE ADDRESSED UNDER THIS SUBMISSION	**5**
4.1	THE CONTINUED EFFECTIVENESS OF THE SCHEME, TAKING INTO ACCOUNT CHANGES IN THE USE OF TECHNOLOGY SINCE THE PASSAGE OF THE BILL	6
4.2	NON-INDEPENDENT GOVERNANCE – INWARD LOOKING OVERSIGHT BY THE EXECUTIVE BRANCH OF GOVERNMENT	21
4.3	POTENTIAL IMPROVEMENTS TO OVERSIGHT, INCLUDING IN RELATION TO JOURNALIST INFORMATION WARRANTS	24
4.4	DEVELOPMENTS IN INTERNATIONAL JURISDICTIONS SINCE THE PASSAGE OF THE BILL	27
5.	RECOMMENDATIONS	**37**
5.1	The Location Information Warrant - Proposed Procedure	37
6.	CONCLUSION	**43**

1. Introduction

Location information (LI) of a cell phone is used when making and receiving SMS', voice calls, browsing the internet and accessing social media applications, from maps to dating to shopping. This is enabled by the location services functionality in the 4G or 5G telecommunications network. The radio signals collect and transfer the estimated location from the cell tower via a gateway to these applications. These applications are referred to as location services clients.[1]

This submission will therefore focus on the generation, storage, collection and use of LI by Telco's, Internet Service Providers (ISPs), the Australian Security and Intelligence Organisation (ASIO) and the Australian Federal Police (AFP), under the *Data Retention Act 2015* (Cth).

Regarding the ***methodology***, to conduct this research: we collected, studied, interpreted and analysed various laws, policies, court cases, parliamentary submissions, technical documents and academic literature. Sections of this research was conducted as part of the PhD research of the author while at the University of New South Wales (UNSW) Sydney (Law School) and Canberra (Australia Centre for Cyber Security [ACCS], School of Engineering and IT), at Australian Defence Force Academy (ADFA) campus, and as a scholarship recipient of the Data to Decisions (D2D) CRC, from 2014 to 2018. The research was peer reviewed and led to peer reviewed research publications,[2] with a book project under way with Springer Nature Switzerland.

The submission is structured as follows:

Part 4.1 will highlight the recent developments in estimating the location of a mobile device with greater precision, from 4G to 5G mobile technologies. In Part 4.1.6 the submission critically analyses how the broad term 'security' has been accepted by Australian courts, thereby confirming the government's sole discretion to decide what activities qualify as threats to national security, without needing clear guidelines to justify its decision. Given this, Part 4.1.7 highlights how young people that protest inaction on the environment are potentially at risk of being targeted under the data retention scheme on the basis that their political actions pose a threat to the national economic interest, especially given the Adani coal mine. Part 4.2 highlights how moving ASIO from the Attorney-General's Department (AGD) and moving the AFP to the portfolio of the Minister of Home Affairs, creates uncertainty about previous governance and accountability frameworks - this requires public clarification. Part 4.3 highlights how the warrant process for journalist sources was bypassed and how the process can be strengthened. Part 4.4 shows how courts in the United Kingdom (UK) and the United States of America (USA) enforced its judicial roles, to ensure oversight over the collection of telecommunications data and location information. Part 4.4. also discusses how Australia is one of the major Western democracies lagging behind in this regard, by not requiring a judicial warrant to access and use location information. Part 5 therefore recommends the introduction of an independent judicial authority, with administrative processes to grant location information warrants.

[1] Shanapinda, S. 2018. Advance metadata fair: The retention and disclosure of location information as metadata for law enforcement and national security, and the impact on privacy – An Australian story, (PhD Thesis). UNSW Canberra University (unpublished).

[2] See: La Trobe University. https://scholars.latrobe.edu.au/display/sshanapinda

2. About the La Trobe University Optus Cybersecurity Research Hub

The La Trobe University Optus Cybersecurity Research Hub thanks the PJCIS for the opportunity to present our research on this subject for this review.

The La Trobe University Optus Cybersecurity Research Hub is a cross-disciplinary research hub, established in 2018 and sponsored by Optus. The hub studies and lectures on cybersecurity, telecommunications, law and policy.[3] Members of the hub have multiple relations with industry and other local and international research institutions, such as CRCs and associations.[4] The hub and its members participate independently in debates and discussions on current technology, political and social issues, on various media and platforms. The views expressed are our own, based on our research, and are not those of our sponsors or affiliates.

3. Executive Summary

Existing 4G and recently launched 5G mobile cellular communication services use small cells with a radius capability of between centimetres, 1m, 100m and 500m. This creates a dense network of cells that are tracking every movement of a mobile device. Previous networks used bigger cells, with a radius of between 70km and 30km. To approximate the location of the mobile phone in the traditional cell tower was therefore challenging, requiring triangulation. With 4G and 5G, location precision is improving and becoming more accurate, with a precision of centimetres.

Added to this, 2018 statistics show that mobile communications are ever more popular amongst young people than amongst the older generation. Given this popularity, the exclusion that location information may only be stored at the start and end of a communication is not effective and meaningful at protecting individual privacy and personal information. Given location precision and the frequency with which mobile communications and multiple internet devices are used by young people the exclusion serves no meaningful privacy protection purpose. Young people, also referred to as digital natives, are also becoming more politically savvy, using social media to organise and protest. This was demonstrated earlier this year, when young people took off

[3] La Trobe University. https://www.latrobe.edu.au/research/centres/technology/cyber-security; https://www.latrobe.edu.au/research/centres/technology/cyber-security/research-themes.

The research conducted for this paper was done as part of the authors PhD thesis during 2014 – 2018, at UNSW Canberra (ADFA). The Optus La Trobe Cyber Security Research Hub is funded by Optus, a mobile telecommunications company. The research is conducted independently and does not reflect the views of Optus.

The author of this submission may be contacted as follows:

Dr. Stanley SHANAPINDA (B Juris, LLB, MM ICTPR, PhD Computer Science [UNSW ADFA]), RESEARCH FELLOW, College of Science, Health and Engineering, School of Engineering and Mathematical Sciences, Department of Computer Science and IT, Optus La Trobe Cyber Security Research Hub, La Trobe LawTech Member, La Trobe Cyber & Networking (C&N) Research Group, Room 211A Building PS1, La Trobe University, Bundoora | Victoria 3086, E: s.shanapinda@latribe.edu.au T: 03 9479 3721| W: https://scholars.latrobe.edu.au/display/sshanapinda, CRICOS Provider 00115M

[4] La Trobe University. https://www.latrobe.edu.au/research/centres/technology/cyber-security/staff

from school to protests inaction on climate change - demanding that the Adani coal mine be stopped. Senior members of the government have labelled the protest actions of the young people and the Greens, an opposition political party, as threats to national security and the national economic interests, openly in national media. More precise location information from 4G and 5G networks, that reveal personal information, are collected to enforce laws and to safeguard the national interest, but without judicial warrants. Given these public statements from the Prime Minister, tech-savvy and politically savvy young people and political parties are put at risk of being investigated based on their free and democratic right to protest policies that are not environmentally friendly. These statements have a chilling effect on the right of young people and opposition parties to participate in political activity, and to organise to that effect. These two groups are becoming more and more politically active in calling for urgent action on climate change, which means that a project such as the Adani coal mine may need to be stopped altogether. Stopping the Adani, coal mine may have impactful economic consequences. The alternative policies of the Greens may be regarded as threats to national security and national economic interest. This places young people and political parties at risk of being identified as persons of interest for national security, for their protest actions being inquired into and investigated. As such, their location information and other 'metadata' may be collected and used for such inquiries and investigations. The possibility that this exists and the statements by the Prime Minister and members of Cabinet, is a threat to the democratic values – the right to free speech, freedom of expression, free debate and the right to protests. Regarding journalist and whistleblower protections, the metadata of the journalist is divorced from and not made the only basis for having to obtain a journalist information warrant. The submission proposes that even if the journalist's metadata is not needed to identify the source, but other means exists to identify the source, the AFP must still obtain the JIW if it intends to identify the source. In this manner, the source is protected – no metadata may be obtained without a JIW if the aim is to investigate secrecy laws and to identify sources. The executive arms of all three United States (US), the United Kingdom (UK) and Australian governments appear intent on keeping the power to collect and use telecommunications data, commonly referred to as 'metadata', in the executive branch of government, away from judicial oversight. However, in 2018 courts in the UK and the US have responded and affirmed their judicial oversight roles, to issue approvals before the data is collected. The question is when Australia will follow suit and not be the outlier Western democracy. To ensure the democratic right to protest free from the fear of surveillance, aided by big data analytics and artificial intelligence capabilities, this submission proposes that Ministerial guidelines and surveillance laws be amended and that a location information warrant process be introduced, whereby warrants are issued by an independent judicial authority.

4. The terms of reference addressed under this submission

This submission will address the following three of the Committee's Terms of Reference:

- the continued effectiveness of the scheme, taking into account **changes in the use of technology** since the passage of the Bill, in Part 4.1 of the submission;
- any potential **improvements to oversight**, including in relation to **journalist information warrants**, in Parts 4.3 and 5 of the submission**;** and
- developments in **international jurisdictions** since the passage of the Bill, in Part 4.4 of the submission.

4.1 THE CONTINUED EFFECTIVENESS OF THE SCHEME, TAKING INTO ACCOUNT CHANGES IN THE USE OF TECHNOLOGY SINCE THE PASSAGE OF THE BILL

Taking into account the continuing changes in the use of mobile technology since the passage of *Telecommunications (Interception and Access) Amendment (Data Retention) Bill* (Cth) in 2015, it is clear that the scheme does not effectively protect the privacy and personal information of tech-savvy young people and political opponents. Given the use of small cells in current 4G and future 5G mobile cellular communications, and the ever-rising popularity of the use of mobile communications amongst young people as recorded in the 2018 period, the 'metadata' retention scheme places ever greater privacy risk particularly on the privacy of young people and political parties, when protesting and opposing projects such as the Adani coal mine and proposing alternative policies. These privacy risks persist despite the legal limitation that location information and other 'metadata' may only be collected at the start and end of the Voice, SMS, email, chat, forum, social media communications.

4.1.1 Location Precision and 5G Small Cells

4G mobile cellular services use femtocells or small cells to connect the mobile phone for Voice, SMS, email, chat, forum, social media communications. The small cell is contained inside the bigger macrocell of the tower. Small cells are located inside homes and near buildings, similar to Wi-Fi hotspots. This is illustrated in Figures 1 and 2 below.[5]

[5] Shanapinda, S. 2018. Advance metadata fair: The retention and disclosure of location information as metadata for law enforcement and national security, and the impact on privacy – An Australian story, (PhD Thesis). UNSW Canberra University (unpublished).

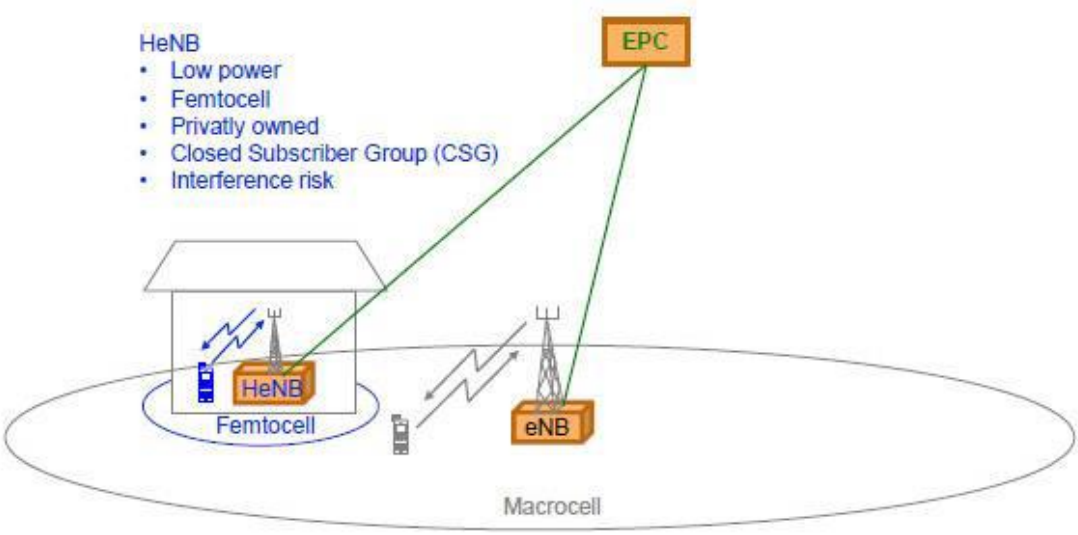

Figure 1 Small cells used in the 4G network[6]

The aim of the small cell is to boost the signal of the bigger macrocell.[7]

Telstra started rolling out 5G mobile cellular communications in May 2019.[8] Similarly to 4G, 5G also uses small cells. These cells are generally located within distances of 100-500 meters.[9] This is also illustrated in Figure 1 below.

[6] Magdalena Nohrborg, LTE, (2017), 3GPP. http://www.3gpp.org/technologies/keywords-acronyms/98-lte

[7] Shanapinda, S. 2018, PhD Thesis, pp. 113-118, 178.

[8] Australia's first 5G service goes live. May 22, 2019 https://www.ericsson.com/en/news/2019/6/5g-live-in-australia-with-telstra

[9] GSMA.pg. 34 Road to 5G: Introduction and Migration. April 2018. https://www.gsma.com/futurenetworks/wp-content/uploads/2018/04/Road-to-5G-Introduction-and-Migration_FINAL.pdf ; 2018 SCTE•ISBE and NCTA. Pg. 17. 5G Small Cells and Cable Realizing the Opportunity A Technical Paper prepared for SCTE•ISBE by Dave Morley

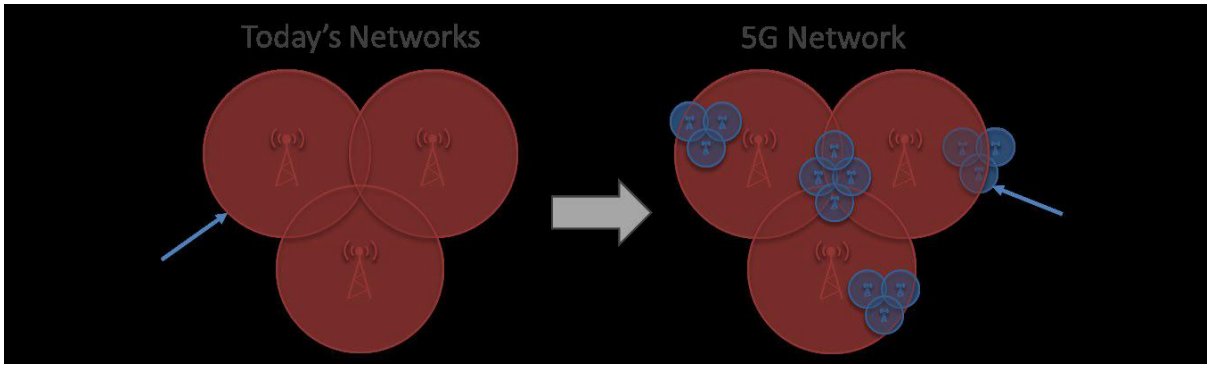

Figure 2 Figure 2 5G Network Densification[10]

This creates a dense network of cells, as indicated in the second graphic of Figure 2. This increase in the number of cells to track the location of the mobile device leads to greater location precision.[11] The location estimates are not as raw and unprocessed as claimed by law enforcement agencies when the Bill was originally introduced, despite indications by the Electronic Frontiers Australia (EFA) that location estimates are becoming more precise.[12] The NSW police stated:

> *With cell site location that we would normally get with metadata, we would talk about an area, for example if I am in Canberra I might be in Deakin or I might be somewhere—it does not specify. There is not the amount of specificity to say that I am in a particular place. We are talking about more gross data.*[13]

The network uses the GPS and other global satellite tracking technologies, to estimate the location of the device with greater precision. The location of the mobile phone and indirectly the location of the user within a 100m sized cell is more precise than a 30km macrocell tower that is generally used by 4G, as illustrated in the first graphic of Figure 2 above. With 5G, estimating the location becomes even more precise – this is one of the improvements ushered in by 5G. As such, location precision may be reduced to 1m or in centimetres.[14] This is significantly better than what current 4G location estimates provide. Current estimates use GPS and other satellite technologies, referred to as Global Navigation Satellite System (GNSS). However, current GNSS capability only has an accuracy of 5m and wireless local area networks that have an accuracy of 3-4m.[15] This

[10] Dave Morley. SCTE ISBE and NCTA. Pg. 9, 17. 2018. 5G Small Cells and Cable Realizing the Opportunity A Technical Paper prepared for SCTE•ISBE. https://www.nctatechnicalpapers.com/Paper/2018/2018-5g-small-cells-and-cable-realizing-the-opportunity/download

[11] Shanapinda, S. 2018, pg. 178. (PhD Thesis)

[12] Ibid

[13] Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 30 January 2015, 48 (Assistant Commissioner Malcolm Lanyon, Commander, Special Services Group, New South Wales Police Force), cited in Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, (27 February 2015), 95 [3.86].

[14] M. Koivisto, A. Hakkarainen, M. Costa, P. Kela, K. Leppanen and M. Valkama, "High-Efficiency Device Positioning and Location-Aware Communications in Dense 5G Networks," in IEEE Communications Magazine, vol. 55, no. 8, pp. 188-195, Aug. 2017. doi: 10.1109/MCOM.2017.1600655; NGMN 5G white paper, [online] Available: https://www.ngmn.org/uploads/media/NGMN5GWhitePaperV10.pdf; 5G Vision, [online] Available: https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf; 5G white paper: New Wave Towards Future Societies in the 2020s, [online] Available: http://kani.or.kr/5g/whitepaper/20155GForumWhitePaperService.pdf; "Study on Scenarios and Requirements for Next Generation Access Technologies (V1.0.0)", 3GPP TR 38.913, [online] Available: http://www.3gpp.org/DynaReport/38913.htm

[15] Ibid

improvement to 1m or centimetre precision unlike existing satellite technology only makes 5G very attractive for use in tracking vehicular traffic, and such vehicular applications are being researched, and may be adapted for use in mobile cell phone applications as well, as location service clients.[16] Location precision is enabled using smart antenna's that focusses in on the device to deliver the radio signal, creating a line of sight position. The 5G network becomes more device-centric as a result.[17]

This development allows for more personal and sensitive information to be revealed. This can be achieved even with the legal exclusion that location information only be collected and stored at the start and end of the communication. For example, the fact that a person was at a protest will be zoomed in to, as a matter of certainty, as opposed to counter arguing that the individual was simply an observer.

4.1.2 The types of Location Information

Location information includes:[18]

i. The location information used to deliver a Short Message Service (SMS) message or a voice communication to the mobile device;[19]

ii. The location information not used to deliver the SMS or voice communication to the mobile device, in other words, the neighbouring or Enhanced cell-ID (E-CID);[20]

iii. The location information generated prior to, during and after a voice or SMS communication;

iv. The location information generated when the individual is not using the device, also referred to as pings and regular connections that mobile devices make to cell towers;[21]

v. The location information stored by the Telco for any period, for commercial purposes and for purposes to maintain the IP-mediated Long-Term Evolution (LTE) and 5G networks, if the Telco has the location information in its possession;[22] and

vi. The International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) of the mobile device, and similar Universal Integrated Circuit Cards (UICC) mobile device identifiers, for both 4G and 5G, that may be in use.

---

[16] Ibid M. Koivisto et. al.,

[17] Ibid fn. 13

[18] Shanapinda, S. 2018. (PhD Thesis)

[19] *TIA Act 1979* s 187AA (1) item 6.

[20] Revised Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Cth), 2015, 44 [246.]

[21] Ibid

[22] *TA 1997* s 275A, 276, 280, 313(3), 313(4), 313(7); *TIA Act 1979* ss 175–184.

4.1.3 Cybersecurity and Privacy Risks Given Advances in Location Precision Technology – Ensuring Compliance

As regards the cybersecurity of the retained location information, the location precision advantage may leave all users of mobile devices more exposed. Location information is also important for law enforcement, national security protection and espionage by state adversaries. The value of location information was demonstrated by recent media reports that global 4G telecommunications companies (Telco's) were hacked by Chinese hackers, which included the 'geo-location of users'.[23]

Under 5G, given that it will mainly be a cloud-based, this creates cybersecurity risks for the software deployed throughout the network, whether in the new radio access part or the core part of network.[24]

Advances in location precision potentially places various groups under privacy risks: i.) women exposed to family violence; and ii.) risks of hacking and leaking the precise locations of police, military personnel and political leaders, when using 5G enabled communications technologies. The risks posed by location aware technologies may therefore have a chilling effect on the behaviour of these groups of persons.

Telco's are required to safeguard the confidentiality, integrity and availability of the network and the information under the data retention scheme.[25] Given these risks, under their legal duty to keep the retained location information secure, Telco's may need to continuously review their security posture to ensure trustworthy levels of security and control, with the full commercial roll out of 5G. The PJCIS may confidentially request the Telco's to demonstrate how they intend on updating their security posture in ensuring compliance with this legal duty.

4.1.4 Mobile Services are Popular with Young People than the Elderly

Mobile phones remain the most popular form of communication used to access social media apps for chats and voice calls in Australia. Generally speaking, the use of mobile phones increased from 93% in May 2014 to 96% in May 2018.[26] An ever-increasing number of Australians rely solely on their mobile phone for voice communications.[27] Eighty-three per cent of Australians only used their smartphones to go online.[28] Seventy-nine per cent (approximately 15.2 million) accessed the internet via a mobile phone. Previously only 75 per cent (approximately 14.4 million) accessed the internet via a mobile phone, in the six months to June 2017.[29]

---

[23] Cybereason Nocturnus. Operation Soft Cell: A Worldwide Campaign Against Telecommunications Providers. June 25, 2019. https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers; Forbes. Zak Doffman. Jun 25, 2019, 12:09am. China's Hackers Accused Of 'Mass-Scale Espionage' Attack On Global Cellular Networks. https://www.forbes.com/sites/zakdoffman/2019/06/25/chinese-government-suspected-of-major-hack-on-10-global-phone-companies-reports/#68ef27c932da

[24] Ericsson. https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system

[25] Section 187BA Telecommunications (Interception and Access) Act 1979 (Cth).

[26] ACMA. Pg. 54 Communications report 2017–18. https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/Communications-report-2017-18-pdf.pdf?la=en

[27] Ibid Pg. 56

[28] Ibid Pg. 54

[29] Ibid Pg. 57

Age continues to be a strong predictor of the popular use of technology. The digital divide is that older Australians use traditional communication services, and younger groups increasingly communicate by using over-the-top (OTT) services. Young people that are aged between 18–44, representing 89% are more likely to use a mobile phone to access the internet multiple times a day than those aged 45 and over, representing 56%.[30] By May 2018, 79% of Australians aged 65 and over, used a fixed-line phone. In contrast, only 18% of young people, aged between 25 and 34 used a fixed-line.[31] Ninety per cent of Australians that are aged between 18–34 use social networking and messaging/calling apps. In contrast, only around a quarter of those aged 65 and over, use OTT services.[32]

Internet users are using multiple devices, and frequently throughout the day. By May 2018, the mobile phone was the most popular device used by 87% of people. The laptop comes in second with 72% and tablets come in third with 61%.[33] By May 2018, 73% of those accessing the internet used their mobile phone multiple times a day to access the internet and 81 per cent used it to go online at least once a day.[34] To better protect privacy, there is however a limit to when location information and other 'metadata' should be collected, as discussed below. The question is how meaningful this privacy safeguard is.

4.1.5 The 'Metadata' Retention and Disclosure Exclusions

The data retention and disclosure scheme aims to protect the privacy of the young people with the flexible legal limit that location information and other 'metadata' should only be collected at the start and end of the Voice, SMS, email, chat, forum, social media communication. There is therefore a restriction to the volume of location information and other 'metadata' that may be collected, stored and therefore handed however to the law enforcement and national security Agencies. The law states:

> *[Section] 187AA Information to be kept*
>
> *(1) The following table sets out the kinds of information that a service provider must keep, or cause to be kept, under subsection 187A(1):*

4	*The date, time and duration of a communication, or of its connection to a relevant service*	*The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication):* *(a) the **start** of the communication;* *(b) the **end** of the communication;* *(c) the connection to the relevant service;*

[30] Ibid Pg. 58

[31] Ibid Pg. 54-55

[32] Ibid Pg. 55

[33] Ibid Pg. 58

[34] Ibid Pg. 58 - 60

		(d) the disconnection from the relevant service.
6	*The location of equipment, or a line, used in connection with a communication*	*The following in relation to the equipment or line used to send or receive the communication:* *(a) the **location of the equipment** or line at the start of the communication;* *(b) the **location of the equipment** or line at the end of the communication.* *Examples: **Cell towers**, Wi-Fi hotspots.*

(emphasis added)[35]

A mobile device constantly communicates with the cell tower and the small cells in the 4G and 5G networks. The location of the device needs to be constantly tracked to be able to deliver the communications to the phone and for the Telco to bill the customer for the services. Even when the 'metadata' is not used for billing the location information is still tracked and stored in the network of the telco.[36] However, the law requires that the location information generated at the start and at the end of a 'Voice, SMS, email, chat, forum, social media' be retained.[37]

5	*The type of a communication or of a relevant service used in connection with a communication*	*The following:* *(a) the type of communication;* *Examples: **Voice, SMS, email, chat, forum, social media**.*

(emphasis added)38

This limit may be referred to as an exclusion: it aims to exclude the retention of location information generated at any other time than at the start and end of the social media communication or voice call. The question is how effective the exclusion is in protecting privacy, given the popular use of mobile services amongst young people, especially those who are politically active. In analysing the usage patterns for mobile communications in relation to the exclusion to only record and store location information at the start and at the end of a Voice, SMS, email, chat, forum, social media communication demonstrates that the exclusion is rather ineffective. Australians and residents are tracked, and their locations are stored most of the times, and there is no meaningful limit that this exclusion has on preserving the privacy of any person using mobile communications, given its popularity. Ninety-two per cent of Australians aged 18–24 accessed the internet three or more times

[35] Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth)

[36] S. Shanapinda 2018 (PhD Thesis, unpublished)

[37] Ibid Section 187AA(1)[5]

[38] Ibid

a day. On the other hand, only 43% of those aged 65 and over, used the internet three or more times a day.[39] The mobile phone is also the most frequently used device to access the internet.[40] For three or more times a day, seven days a week, and over various internet devices the location information and other 'metadata' are collected and stored. This is true for 92% of young people.

Additionally, the exclusion safeguard is ineffective because location information may still be collected prior to, during and at the end of the Voice, SMS, email, chat, forum, social media communications. The Telco is not strictly prohibited from doing so. Telco's may need to store more information for maintenance and other commercial purposes. If the Telco has the information available the Telco may be requested to share the information, or even do so voluntarily. The agencies are also not prohibited to only collect location information stored at the start and at the end of the communications. There are no legal penalties for either the agencies or the Telco's if they were to collect, store, disclose and use location information prior to, during and after the communications ended.[41]

The location information is stored, collected and used for law enforcement and national security purposes. The mobile internet is 'part of the DNA' of young people. It is a basic activity that is normal and innate to them. The surveillance laws have the impact of indirectly forcing young people to give up their lifestyles if they do not wish to be surveilled, their locations tracked, their profiles generated and stored and handed over to ASIO and the AFP. This surveillance risk is instilled in the name of broad umbrella terms such as: 'security', 'law enforcement' and 'public safety'. Under these broad terms, the organiser of a protest demanding better protect for the environment, may be considered a threat to national security, given the importance of coal to the economy and job creation. The terms 'security' and 'national security' are so broad that protests activities by young people and political opponents have already been described as threats to national security, as discussed in Part 4.1.7. The likely legal impact and the potential surveillance impact that may arise from these political statements are discussed below.

4.1.6 Defining the Term 'Security'

According to the Attorney-General's Guidelines, ASIO conducts its investigations, assessments and inquiries into 'activities relevant to security'[42] or 'activities prejudicial to security'.[43] The term 'security' is broad term may include the economic interests of the country, as discussed in Part 4.1.7. National security means '…Australia's defence, security or international relations.'[44] International relations means '…political, military and economic relations with foreign governments and international organisations.'[45]

---

[39] ACMA. Pg. 58 Communications report 2017–18. https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/Communications-report-2017-18-pdf.pdf?la=en

[40] Ibid

[41] S. Shanapinda 2018 (PhD Thesis, unpublished)

[42] Attorney-General's Guidelines 4.1(a) https://www.asio.gov.au/sites/default/files/Attorney-General's%20Guidelines.pdf

[43] Ibid 4.1(b)

[44] *Security of Critical Infrastructure Act 2018* (Cth)

[45] Ibid

Security also includes acts of sabotage: 'Note 1: Security, among other things, covers the protection of, and of the people of, the Commonwealth and the States and Territories from espionage, sabotage, attacks on Australia's defence system and acts of foreign interference.'[46]

Security also means:

> *(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:*
>
> *(i) espionage;*
>
> *(ii) sabotage;*
>
> *(iii) politically motivated violence;*
>
> *(iv) promotion of communal violence;*
>
> *(v) attacks on Australia's defence system; or*
>
> *(vi) acts of foreign interference;*
>
> *whether directed from, or committed within, Australia or not;*[47]

Also, under the *Assistance and Access Act 2018* (Cth), ASIO, AFP and the Australian Defence Force (ADF) via the Australian Signals Directorate (ASD) may collect relevant data from social media organisations, Telco's and ISPs, to safeguard national security and Australia's national economic well-being:

> *(5) For the purposes of this section, relevant objective means:*
>
> *(a) in relation to a technical assistance request given by the Director-General of Security—safeguarding national security; or*
>
> *(b) in relation to a technical assistance request given by the Director-General of the Australian Secret Intelligence Service—the interests of Australia's national security, the interests of Australia's foreign relations or the interests of Australia's national economic well-being;'*[48]

The *Assistance and Access Act 2018* (Cth) clearly links the economy and activities that may impact the economy to national security. This blurs the lines between where national security starts and where the economy ends, as these interests are seen as joint. This creates uncertainty as to how these terms may be interpreted and applied in practice, creating surveillance risks for politically and tech-savvy young people and for political opponents.

[46] subsection 313(1) (1A) *Telecommunications Act 1997* (Cth); Section 8 *Telecommunications and Other Legislation Amendment Act 2017* (Cth)

[47] Section 4 *Australian Security Intelligence Organisation Act 1979* (Cth)

[48] Section 317E(2)(iii), 317G(5), Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth); section 34AAA (2)(vi) Australian Security Intelligence Organisation Act 1979

4.1.6.1 The Courts Accept the Wide Definition of 'Security'

Courts have been reluctant to limit the definition of 'national security' and recognised the discretion of the executive branch of government to decide what is in the national interest to safeguard national security. The courts have generally allowed the government to decide what it considers to be a matter of national security. The next Part discuss how the courts refused to limit the meaning of the term 'security', thereby confirming the broad powers of the government to decide what actions qualify as a threat to national security, but with no clear prior guidelines to take such a decision.

4.1.6.1.1 Farrell; Secretary, DIBP (Freedom of information)

In the case: Farrell; Secretary, Department of Immigration and Border Protection (Freedom of information)[49] the court rejected the assertion that the term 'security of the Commonwealth'[50] should be confined only to activities of a warlike nature, even after acknowledging that the term is one that fluctuates.[51]

4.1.6.1.2 Jaffarie v Director General of Security

In the case: Jaffarie v Director General of Security,[52] Mr Jaffarie alleged that the Director-General of ASIO erred in his construction and application of the term 'security'.[53] Mr Jaffarie challenged the interpretation of the word 'security', arguing that the meaning must be confined.[54] Honourable Justices Flick and Perram decided against Mr Jaffarie,[55] stating that the Commonwealth legislature is not limited to adopt a confined meaning of the term 'security'.[56]

The Jaffarie case concluded: a confined meaning of 'security' would be a high bar and frustrate the ability of ASIO to properly monitor and assess threats.[57] The Jaffarie case notes that Parliament rightfully uses the term security, despite an objection that it may be too broad. The case indicates there was no misuse of power under the guise of 'security'. In respect of collecting location information about the individual, further precaution may need to be taken, given the broad meaning of 'security' and the confidential nature of the investigations of the Agencies. Greater privacy protection, such as a requirement for the prior approval of a third party for access to or use of location information, may be an appropriate safeguard.

---

[49] [2017] AATA 409 (31 March 2017).

[50] Freedom of Information Act 1982 (Cth) s 33(a)(i).

[51] Farrell; Secretary, Department of Immigration and Border Protection (Freedom of information) [2017]

[52] [2014] FCAFC 102 (18 August 2014).

[53] Ibid [52].

[54] Ibid 20 [54].

[55] Ibid 24 [66], 39 [116].

[56] Ibid 23 [64], 21 [59]. Also see *RZBV and Director-General of Security and Anor* [2015] AATA 296 (5 May 2015) 7 [17].

[57] Ibid 23–24 [65] cited *Suresh v Canada (The Minister of Citizenship and Immigration)* [2002] SCC 1 at [88], [2002] 1 SCR 3, 50–51.

4.1.6.1.3 Church of Scientology Inc v Woodward

In the case: Church of Scientology Inc v Woodward,[58] Mason J stated: '… security is a concept with a fluctuating content, depending very much on circumstances as they exist from time to time.'[59] The meaning of 'security' is not fixed but is unpredictable.

The courts are likely to dismiss any challenge that the powers of ASIO to collect location information for security reasons are too broad, despite the imprecise and fluctuating meaning of the term 'security'. The question is how privacy is best protected under these circumstances. The answer clearly does not lie with challenging the broadness of the power based on what the terms 'national security', 'security', 'activities relevant to security'[60] and 'activities prejudicial to security'[61] mean, and to try and limit their meaning. The answer may lie with how location information and other 'metadata' is collected in the first place, to enable an investigation and an inquiry into 'activities relevant to security'[62] or 'activities prejudicial to security'.[63] As such, the Location Information Warrant (LIW) is proposed in Part 5. Young people are becoming more politically active. As discussed below, their activities are at risk of being equated to being 'activities relevant to security'[64] and 'activities prejudicial to security'.[65] The position of courts and the broad definition of 'security' potentially makes young people, climate change activists and the Greens political party and their leadership and membership, protesting the closure of the Adani coal mine a threat to national security.

4.1.7 Young People Become More Politically Active in Recent Months

Since the Occupy Sydney protests in 2011,[66] in March 2019 young people have taken to the streets, this time to protest climate change, a politically sensitive issue.[67] It seems young people will continue to protest in future.[68] Young people have also taken their views to national television.

4.1.7.1. Climate Change and the Adani Coal Mine as National Security Issues

On the QandA TV talk show that aired on the ABC on Monday 15 April 2019, at 9:35pm, climate change and the Adani coal mine were discussed. The Adani coal mine project is a project with great national economic value and therefore of national economic interest, despite its potential negative impact on the environment - it is stated the project will provide much needed jobs in Queensland, and for this reason the project must go ahead. This is because a project such as this, is said to be '…about securing Australia's future'.[69] Senator

---

[58] [1982] HCA 78; (1982) 154 CLR 25

[59] Ibid 60

[60] Attorney-General's Guidelines, 4.1(a)

[61] Ibid 4.1(b)

[62] Ibid 4.1(a)

[63] Ibid 4.1(b)

[64] Ibid 4.1(a)

[65] Ibid 4.1(b)

[66] ABC. Despite arrests, Occupy protesters won't give up Updated 24 Oct 2011, 1:33pm https://www.abc.net.au/news/2011-10-24/occupy-protesters-vow-to-continue/3597178

[67] The Conversation. Hannah Feldman. Young people won't accept inaction on climate change, and they'll be voting in droves. May 2, 2019 5.55pm AEST. https://theconversation.com/young-people-wont-accept-inaction-on-climate-change-and-theyll-be-voting-in-droves-116361 ; Climate change strikes across Australia see student protesters defy calls to stay in school. Updated 16 Mar 2019, 12:02am https://www.abc.net.au/news/2019-03-15/students-walk-out-of-class-to-protest-climate-change/10901978

[68] Ibid

[69] ABC. Election 2019: The Battle For Queensland. https://www.abc.net.au/qanda/2019-15-04/10988470

James McGrath, Liberal Senator, in his official capacity as Senator, highlighted the Adani project as being of national security interest because of its economic significance. Below is an extract from the show:

> *ETHAN MOLDRICH*
>
> *Thanks, Virginia. My question is to Senator McGrath. Does the LNP have a plan to win over* ***Liberal-minded young people who oppose Adani*** *and offshore detention, but support the Coalition's economic plan? Or is the LNP ceding these votes to other parties this election?*
>
> *LARISSA WATERS*
>
> *Great question.*
>
> *JAMES McGRATH*
>
> *In terms of what the Liberal National Party, in terms of our pledge and our manifestos and* ***our values that we're taking to the coming election is based on what Scott Morrison, as the leader of the Liberal Party, and Michael McCormack, as leader of the National Party, are talking about, and that's about a stronger future, and it's about securing Australia's future.*** *That's why we've got a range of tax cuts, that's why we've got a range of...of* ***infrastructure projects coming to Queensland****.*
>
> *In terms of* ***Adani****, you've heard me answer that question before in terms of that* ***I'll always support jobs, especially in regional Queensland****. And I think it is wrong to use Adani as... which the panel has already sort of sussed, as an exemplar, in terms of other issues.* ***Adani*** *is a project that will deliver to parts of Queensland that don't have the wonderfulness of Brisbane and, say, the Sunshine Coast and the Gold Coast.* ***It will deliver jobs to disadvantaged communities****.*
>
> *VIRGINIA TRIOLI*
>
> *James, I'm just going to jump in, because the question actually... The questioner said* ***Adani is something that he opposes****, so you're not going to be able to persuade him tonight.*
>
> *JAMES McGRATH*
>
> *I know. What I'm trying to do... And what I'm trying to do is say that...that* ***Adani's actually more than just a coalmine. It's about helping people get on****. And for* ***those who are liberally minded, the best way, I think, you can help people get on with life is actually having a job****, in terms of* ***helping breaking that welfare cycle*** (emphasis added).[70]

The gist of the extract is that the questioner opposes the Adani coal mine project, demonstrating his political activity and liber-minded ideology, as is normal in a free and democratic society. However, the project is politically seen as a national security issue. The question is what this legally means with regards to the possible collection and use of the location information and other 'metadata' of the caller, that opposes a project that is politically seen as being of national economic interest.

The Greens political party also opposes the construction of Adani, lobbying that it be stopped altogether.[71]

---

[70] Ibid

[71] The Greens Queensland. The Plan to Stop Adani.2019. https://greens.org.au/qld/platform/plan-to-stop-adani

4.1.7.2 The Greens Political Party Activities are Described as a National Security and Economic Threat to Australia

Senator McGrath stated above that '…our [the Liberal Party] values that we're taking to the coming election is based on what Scott Morrison, as the leader of the Liberal Party, and Michael McCormack, as leader of the National Party, are talking about, and that's about a stronger future, and it's about securing Australia's future.'[72] The Senator and the Prime Minister described the political activities about climate change by young people and political parties, such as the Greens, in April and May 2019 as threats to national security and the national economy. In May 2019, the as leader of the Liberal Party and as the Prime Minister, Mr. Morrison seem to have suggested that these protest activities are an issue of national security. Mr. Scott Morrison warned that the Greens political party are a threat to economic and national security, by opposing the Adani coal mine project. The news reports quoted Mr. Morrison as saying:

> *"The Greens represent the greatest* ***threat (to the economy and national security****), and the Labor Party only moves closer and closer and closer to the Greens,"*[73]
>
> And,
>
> *"It's* ***infesting their economic policy****, it's* ***infesting their national security outlook****."*[74]
>
> And,
>
> *"… a* ***danger to the economy*** *and they are* ***a danger to national security*** *… I think that is a fairly unremarkable statement,"*
>
> And,
>
> *"****They want to abolish the US -alliance and remove every area of co-operation****. The Greens' agenda has only* ***become more extreme****, particularly over this last term. They are more* ***unabashed*** *when it comes to* ***activism****," he said.'*[75]
>
> And,
>
> *'… the* ***Greens policies pose a clear and present danger to the Australian economy'****.*[76]
>
> And,
>
> *'Mr Morrison told The Weekend Australian that it was* ***weakening Australia's investment future when activists turned any mine into a totemic campaign against all mining and industry****.'*[77] (emphasis added)

[72] ABC. Election 2019: The Battle For Queensland. https://www.abc.net.au/qanda/2019-15-04/10988470

[73] PM Politics. Greens 'a greater threat than Palmer'. 11 May 2019 7:27 am AEST https://www.nationaltribune.com.au/greens-a-greater-threat-than-palmer-pm/

[74] Ibid

[75] Ibid

[76] Ibid

[77] Ibid

The statement about abolishing the US-alliance is about Australia's international relations, which is included in the definition of security.[78]

In terms of the court decisions discussed above, the political statements of the Senator and the Prime Minister are legally acceptable statements – opposing the Adani coal mine and protesting against it, on climate change or ideological bases, may therefore legally be categorised by the government as posing a threat to national security, if the government wanted to, because of its economic and job creation value. The question is what guidelines the government may use to make such a decision, if it wanted to make that decision. This situation sets a dangerous trend and clears the way for a legal basis to inquire into and investigate the actions of politically and tech-savvy young people and opposition political parties under the data retention and disclosure scheme with no prior judicial oversight. This is especially so given how scarce natural resources such as fresh drinking water may become and may need to be managed differently, as evidenced by the Mass fish die-off in the Darling River.[79] Also, in 2010, surveillance concerns were raised about environmental activists who opposed the Victorian desalination plant.[80] Environmental issues thus keep coming up. To bring about water policy reform climate change protests and demonstrations by tech-savvy and 'environmentally-woke' young people may be needed, putting themselves at risk with security authorities given the political statements that equate climate change protests to national security threats. This is critically discussed below.

4.1.7.3 Tech-Savvy and Politically Active Young People are Potential Targets of the Data Retention and Disclosure Scheme

As discussed in Part 4.1.3, young people use more mobile services whereas seniors use more fixed line services, which services are declining. These use patterns indicate that young people are more mobile. Mobility means that their locations are tracked. Given the differences in the usage patterns between fixed and mobile services, it means that young people, their location information, profiles, habits and profiles, personal information and are more at risk of being collected, stored and revealed to ASIO and the AFP than those of senior citizens. This while younger people are showing signs of political activism. This means young people are more at risk simply because they are digital natives, born into the digital age and in an age where fixed-line communications are less popular and foreign to them. The younger generation is therefore put at greater risks by these surveillance laws, simply for using mobile communications that seems 'natural' and obvious to them. It is not simply that they choose to, but because of the ubiquity of mobile communications that is entrenched in everyday living – banking, shopping, ordering meals, travel, dating, spending time with friends and family. Just doing these obvious day-to-day activities that young people take for granted and that have become their way of life exposes them to dragnet surveillance. The question is how free young people are to use mobile communications if they are faced with the risk of surveillance – and have their locations tracked and profiled – versus not living their daily normal life's for fear of being tracked and exposed. These risks get bigger as young people show signs of political activism and use social media applications like WhatsApp and Telegram, and other online communities to discuss climate change, organise protests and marches. Young people are

[78] *Security of Critical Infrastructure Act* 2018 (Cth)

[79] ABC. Sowaibah Hanifie and Nadia Isa. Mass fish die-off in Darling River could impact fish numbers in other states. ABC Riverland. Updated 15 Jan 2019, 4:13pm. https://www.abc.net.au/news/2019-01-15/mass-fish-kill-in-darling-river-to-impact-other-states/10715640

[80] Victorian Government. Inquiry into arrangements for security and security information gathering for state government construction projects. Final report of the Victorian Parliament Law Reform Committee. October 2010. Authority Victorian Government Printer Parliamentary Paper No. 394, Session 2006-2010. https://www.parliament.vic.gov.au/papers/govpub/VPARL2006-10No394.pdf

becoming 'environmentally-woke' because they see how climate change will impact their generation. They therefore demand urgent action to start rolling back the effects of climate change.

Australian young people are therefore likely to be discriminately impacted by Australia's surveillance laws, simply because of their political activism and for being tech-savvy. The statements by the Prime Minister equate political activity and the freedom of expression by opposing a mining project on the basis of climate change, as being a threat to national security. As per the above court decisions, describing a protest action as a threat to national security is possibly in the remit of the government. As such, under the law enforcement and national security laws, the activities of the young people and an opposition political party, does theoretically qualify as 'activities relevant to security'[81] or 'activities prejudicial to security', because 'they pose a clear and present danger to the Australian economy'.[82] Online chats about climate change related to the Adani coal mine would therefore qualify as being of interest to the Australian Defence Force (ADF), ASIO and the AFP. This is because projects such as the Adani coal mine is politically, and therefore may legally, be considered a national security issue given its economic significance. It will have a chilling effect on young people that intend on participating fully in political activities, especially about the environment, for which they demonstrate such passion.[83]

The political statements that equate the right to protests climate change and youth activism the national security threats potentially have the impact of intimidating the political opposition and young people to exercise their political rights. This has a chilling effect on free speech, the right to protests and to express different political views by political parties, counter to what should be the norm in a democratic society and under Australia's international civil and political right obligations under the International Covenant on Civil and Political Rights (ICCPR).

There have not been public reports about the collection of young people's 'metadata' or location information, or those of political parties opposed to the policies of the government. This submission does not imply that this has occurred. This submission simply argues that the actions of young people, that are frequent users of mobile technologies and who are passionate about protesting about climate change inaction, are the likely future targets of the surveillance laws. The actions of these young people and of the political parties are branded as threats to national and economic security. As a result, under these surveillance laws, the 'metadata' of young people and political opponents may be lawfully collected and used, without a judicial warrant, as a means of independent oversight. If those actions were to happen, in future, and were challenged in court, the courts are likely to rule that the exercise of those powers are lawful, despite the lack of independent oversight at the time of collection and use of the 'metadata' of young people and political opponents. The question is whether this state of affairs – if it were to happen under the current laws – would

[81] Attorney-General's Guidelines 4.1(a).

[82] ibid 4.1(b).

[83] In 2016 the AFP announced plans to harvest social media posts.

See: Shanapinda, S. 2018, pg. 178. Advance metadata fair: The retention and disclosure of location information as metadata for law enforcement and national security, and the impact on privacy – An Australian story, (PhD Thesis). UNSW Canberra University (unpublished); Rohan Pearce. (Computerworld). Govt promises $1.6m for AFP big data capabilities Australian Crime Commission receives $1m for new tech. 15 June, 2016 12:36. https://www.computerworld.com.au/article/601764/govt-promises-1-6m-afp-big-data-capabilities/;

ASIO is also harvesting social media posts referring to it as OSINT and using it to analyse it in the national interest.

See: ASIO. How we do it. https://www.asio.gov.au/how-we-do-it.html;

Big Data platforms are developed to predict protests in near real time, to enforce laws and in the national interests.

See: Data to Decisions CRC, 2019. Beat the News. https://www.d2dcrc.com.au/rd-programs/beat-the-news/.

be ok. This submission argues that there must be clear independent oversight guidelines, that are outward looking, under which such surveillance activity may be undertaken in a manner that is more transparent and the rules are clearer, in terms of the legitimate expectations of the public.

4.2 NON-INDEPENDENT GOVERNANCE – INWARD LOOKING OVERSIGHT BY THE EXECUTIVE BRANCH OF GOVERNMENT

The current laws as is written – common, as well as statutory laws, would allow for the collection and use of the location information of the Greens political party and young people, to assess national security threats. There are no explicit legal restrictions nor exclusions that would regulate how such a sensitive investigation would be initiated and be undertaken, and what the clear governance safeguards would be. No government guidelines that are publicly known exists, clearly outlining the circumstances under which these powers may or may not be used.

The *ex post facto* oversight role and the power to exercise security and law enforcement functions are concentrated in the hands of the executive arm of government - the public oversight bodies that are also part of the executive arm of government.[84]

The AFP and ASIO both report to the same Minister of Home Affairs.[85] The surveillance powers are now concentrated in the hands of the Minister of Home Affairs.[86]

The Communications Access Coordinator (CAC), which is located in the same office as the Attorney-General (AG), is the same body that limits the exercise of the AFP and ASIO in terms of the CAC Determination 2015 and the Attorney-General's Guidelines – the limits are to consider the privacy of the individual and only collect location information and other 'metadata' that is justifiable and proportional to the exercise of the powers of the Agencies. These powers are however broad, as indicated by terms such as 'security'.[87]

The AG also has an oversight role, but one that appears limited to the use of special powers: 'The Attorney-General has oversight of ASIO's use of special powers.'[88] Prior to the Minister of Home Affairs overseeing ASIO the Attorney-Generals (AGs') Guidelines, as discussed below, supervised the powers of ASIO to collect and use personal information for their operations. ASIO operations and the handling of emerging security issues are under the mandate of the Minister for Home Affairs. The Attorney-General's Guidelines are not

[84] Keiran Hardy and George Williams, 'Executive Oversight of Intelligence Agencies in Australia', (June 7, 2016) in Goldman, ZK and Rascoff, SJ (eds), Global Intelligence Oversight: Governing Security in the Twenty First Century (2016); UNSW Law Research Paper No. 2016-35, https://ssrn.com/abstract=2804835; Department of Justice, Attorney General's Guidelines On General Crimes, Racketeering Enterprise And Domestic Security/Terrorism Investigations (2 March 2017). https://www.justice.gov/archives/ag/attorney-generals-guidelines-general-crimes-racketeeringenterprise-and-domestic

[85] AFP. About Us. https://www.afp.gov.au/about-us/governance-and-accountability

[86] ASIO. Ministerial and Parliamentary Oversight. https://www.asio.gov.au/ministerial-and-parliamentary-oversight.html

[87] Attorney-General's Department, 'Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)', June 2016. https://www.asio.gov.au/sites/default/files/Attorney-General's%20Guidelines.pdf; Shanapinda, S. 2018, pg. 178. Advance metadata fair: The retention and disclosure of location information as metadata for law enforcement and national security, and the impact on privacy – An Australian story, (PhD Thesis). UNSW Canberra University (unpublished), pg. 113-118.

[88] ASIO. Ministerial and Parliamentary Oversight. https://www.asio.gov.au/ministerial-and-parliamentary-oversight.html

directly referred to as applicable to ASIOs operations and its handling of emerging security issues, to ensure accountability, and no other replacement guidelines have been publicised. It is therefore not clear whether the Minister of Home Affairs has passed similar guidelines to oversee the actions of ASIO and the AFP, with regards to location information and other 'metadata' collection and use.[89] The PJCIS may need to clarify how previous guidelines continue to apply to activities of the Agencies or the replacement guidelines that may have been issued, if any, or any plans in that regard. The submission however assumes that the AGs' Guidelines continue to apply to the collection and use of location information.

4.2.1 Unclear Ministerial Oversight over Operational Activities

Under the Attorney-Generals (AGs') Guidelines and the *ASIO Act 1979* (Cth), ASIO is restricted to undertake investigations where the only basis for the investigation is to investigate the exercise of a person's right of lawful advocacy, protest or dissent.[90] The exception however is that, if the protest falls under the definition of security, ASIO may investigate the said demonstration:

> 16.3 ASIO is **not to investigate demonstrations** or **other protest activity unless**:
>
> (a) …
>
> (b) **it suspects there is a link** between the demonstration or other protest activity and conduct coming otherwise **within the definition of security** (emphasis added).[91]

However, as stated above, the status of these guidelines appears uncertain – the application of these guidelines to the operations of ASIO need to be clarified and confirmed by the Minister of Home Affairs. The statements calling for Adani to be stopped and requiring action on climate change – go against efforts to roll out and commence mining on Adani. In other words, it would stop Adani and have negative economic impacts and negatively affect jobs. The Greens and the students are trying to obstruct the issuing of mining licences to Adani and are doing so for political advantage. Adani is being opposed and would be stopped and for political reasons because coal use in generating electricity is said to cause changes in the climate given the carbon emissions. The statements from the Prime Minister seem to suggest that these protest activities would be issues of security - Scott Morrison warned that the Greens are a threat to economic and national security.[92] The question is whether the activities of the Greens and the young climate change protestors about the Adani coal mine may qualify as acts that fall within the definition of security, based on the political statements by the Prime Minister.[93] This also may need to be clarified – whether these statements were simply political rhetoric or whether the exercise of the right of lawful advocacy, protest and dissent was equated to a security threat, that is likely to attract the collection of the location information and other 'metadata' of the Greens and young people.

---

[89] ASIO. Ministerial and Parliamentary Oversight. https://www.asio.gov.au/ministerial-and-parliamentary-oversight.html

[90] Section 17A *ASIO Act* 1979 (Cth); Section 16.2 Attorney General's Guidelines

[91] Section 16.3(b) Attorney General's Guidelines

[92] PM Politics. Greens 'a greater threat than Palmer': 11 May 2019 7:27 am AEST https://www.nationaltribune.com.au/greens-a-greater-threat-than-palmer-pm/

[93] Ibid

Under the Ministerial Direction issued before the AFP joint the Minister of Home Affairs, AFP does not have the same restriction as ASIO.[94] The question is whether the AFP may investigate and inquire into the exercise of a person's right of lawful advocacy, protest or dissent when the AFP suspects there a link between the demonstration or other protest activity and conduct is coming otherwise within the definition of security. The Ministerial Direction may need to be updated to clarify that this would not be the direction the AFP would take under the Minister of Home Affairs.

Except for violent protests, no other restrictions are placed on the types of acts of political opposition and protests that are likely to qualify as threats to national security. This means the activities of members of the political party and those of tech-savvy young people, who are becoming vocal in this space, may potentially be inquired into and their location information and 'metadata' collected and used, to assess if they pose a threat to national security. There are no publicly known restrictions about the Prime Minister or any member of Cabinet, such as the Minister of Home Affairs referring such acts for inquiry.

ASIO must keep itself free from any influences or considerations that are not relevant to its functions.[95] A referral from a Minister in the government to inquire into the activities of the Greens and young people may qualify as relevant to the functions of the ASIO, because of the link created to national security. ASIO may find it challenging to rebuff the referrals, if such a referral were to be made, on the basis of political interference, if a report is presented as to the negative impacts of stopping the Adani mine, as evidence of the national security link. Any criticism of such a potential inquiry or investigation, where the location information may be collected and used, may be met with a response that the Agencies are simply enforcing current law and that no one is above the law. No clear guidelines exist how the Ministers may take such decisions and how ASIO may respond, and how such a collection of location information and other 'metadata' may be challenged transparently, as would be required in an open and democratic society.

Instead of trusting that political rivals, and the government would always do the right thing, it may be best to introduce clear guidelines and restrictions in this regard. This effort would strengthen the rule of law. Internationally, the United States has the 'Attorney General's Guidelines On General Crimes, Racketeering Enterprise And Domestic Security/Terrorism Investigations' for the Federal Bureau of Investigations (FBI), which are public.[96] These guidelines distinguish between investigations, inquiries and sensitive criminal matters, such as issues involving politicians.[97] For example, the guidelines are clear that the FBI is not allowed to use 'Non-consensual electronic surveillance'[98] for inquiries.[99] The AG's Guidelines and the Ministerial Directions of ASIO and the AFP can be benchmarked against these guidelines, and be improved to set clear boundaries. Stricter standards are also recommended to better safeguard privacy interests, as proposed in Part 5.

---

[94] AFP. About Us. https://www.afp.gov.au/about-us/governance-and-accountability/governance-framework/ministerial-direction

[95] Section 20 *ASIO Act 1979* (Cth)

[96] Department of Justice, Attorney General's Guidelines On General Crimes, Racketeering Enterprise And Domestic Security/Terrorism Investigations (2 March 2017). https://www.justice.gov/archives/ag/attorney-generals-guidelines-general-crimes-racketeering-enterprise-and-domestic

[97] Ibid [A] – [C]

[98] Ibid [B] (5) (c)]

[99] Ibid [B. (5)] – [B. (6)

4.2.2 ASIO Still Yields Tremendous Power, Despite the Privacy Safeguards That Were Introduced in 2015

Privacy is used as a tool to restrict the powers of the Agencies under the data retention and collection scheme. However, the Agencies are simultaneously targeting the private and personal details of the individual. The collection and analysis of location information reveals personal and sensitive information about the individual.[100] The privacy protections are provided for under section 180F.[101] However, the decision to decide how the privacy of the individual is impacted is also left to the discretion of the Agencies.[102] The same Agencies also decide on the activities related to their functions, and based on their public safety interests and strategic directions issued by the executive branch of the government.[103] ASIO thus exercises tremendous power over the personal information of people, and with only executive oversight,[104] which is conducted *ex post facto*. This is however a clear conflict of interests. The Commonwealth Ombudsman and the OIGIS are public oversight bodies that are part of the executive arm of government and not part of the independent judicial branch.[105] The oversight is not conducted in advance, at the time of collection of the personal information by the independent judiciary.[106]

It may be best to ensure that the judiciary approves the warrants that will authorise the collection of location information and other 'metadata' that reveals personal and sensitive information about the individual, as proposed in Part 4.3 below. As discussed earlier, 5G technology will reveal more precise location estimates and in turn easily reveal more sensitive information about the individual.

4.3 POTENTIAL IMPROVEMENTS TO OVERSIGHT, INCLUDING IN RELATION TO JOURNALIST INFORMATION WARRANTS

This Part proposes re-wording the *TIA Act 1979* (Cth), to better protect journalist sources.

4.3.1 Journalist Information Warrants – AFP Officials Are Held to a Different Standard

Section 180H of the *TIA Act 1979* requires the AFP to obtain a JIW to identify a whistleblower. It states:

---

[100] Shanapinda, S. 2018. Advance metadata fair: The retention and disclosure of location information as metadata for law enforcement and national security, and the impact on privacy – An Australian story, (PhD Thesis). UNSW Canberra University (unpublished).

[101] *TIA Act 1979* (Cth)

[102] Ibid pg. 178

[103] Ibid pg. 305

[104] Hardy, Keiran and George Williams, 'Executive Oversight of Intelligence Agencies in Australia', in Goldman, ZK and Rascoff, SJ (eds), Global Intelligence Oversight: Governing Security in the Twenty-First Century (2016); UNSW Law Research Paper No. 2016–35 (7 June 2016). https://ssrn.com/abstract=2804835; Williams, George, 'The Legal Assault on Australian Democracy' (2016) 16(2) QUT Law Review 19

[105] Keiran Hardy and George Williams, 'National security reforms stage one: intelligence gathering and secrecy' (2014) 6 (November) Law Society of NSW Journal (LSJ) 68. https://search.informit.com.au/fullText;dn=20151952;res=AGISPT; Shanapinda, S. 2018, pg. 178, 364-5.

[106] *TIA Act* 1979 (Cth) s 186A; Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 29 January 2015, 41 (Vivienne Thom, Inspector-General of Intelligence and Security, Office of the Inspector-General of Intelligence and Security).

An authorised officer of an enforcement agency must not make an authorisation under section 178, 178A, 179 or 180 that would authorise the disclosure of information or documents relating to a particular person if:

(a) the authorised officer knows or reasonably believes that particular person to be:

(i) a person who is working in a professional capacity as a journalist; or

(ii) an employer of such a person; and

(b) a purpose of making the authorisation would be to identify another person whom the authorised officer knows or reasonably believes to be a source;

unless a journalist information warrant is in force, in relation to that particular person, under which authorised officers of the agency may make authorisations under that section.

By the end of November 2018, the Commonwealth Ombudsman identified AFP's non-compliance in a number of key areas. These included:

- adherence to the Journalist Information Warrant (JIW) provisions;
- inability to sufficiently demonstrate required privacy considerations; and
- access to unauthorised telecommunications data'.[107]

The Commonwealth Ombudsman does not report an issue of non-compliance unless it considers it to be serious: 'We do not generally include administrative issues or instances of non-compliance where the consequences are negligible, for example where the actions of an agency did not result in unnecessary privacy intrusion.[108] According to the Commonwealth Ombudsman: 'Agencies have the power to internally authorise access to this information, however, *if an agency wishes to access telecommunications data that will identify a journalist's information source, the agency **must** apply to an external issuing authority for a warrant*.'[109] AFP officials are required to obtain JIWs to identify sources but are not held accountable, if it fails to obtain JIWs. In April 2017, an AFP official that was investigating a leak obtained the 'metadata' of a journalists without a warrant, as required by the law.[110] The AFP indicated no action was taken against the officer: 'No disciplinary action has been taken against the investigator behind the breach, with Commissioner Colvin saying he did not believe there was any "ill will or bad intent".'[111] The Commonwealth Ombudsman (CO) referred the issue of

[107] Commonwealth Ombudsman. A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979. For the period 1 July 2016 to 30 June 2017. November 2018. Pg. 2. https://www.ombudsman.gov.au/__data/assets/pdf_file/0033/96747/201617-Chapter-4A-Annual-Report.pdf

[108] Ibid Pg. 5

[109] Ibid Pg. 1

[110] Royes, L. 'AFP officer accessed journalist's call records in metadata breach' ABC (online) (29 April 2017) http://www.abc.net.au/news/2017-04-28/afp-officer-accessed-journalists-call-records-inmetadata-breach/8480804

[111] Ibid

non-compliance to Parliament in 2017 and there is no indication of what happened to the referral.[112] In November 2018 the CO reported the latest status as being: 'Through our routine annual inspections of the AFP we continue to monitor the AFP's compliance, including the progress made by the AFP in addressing previous inspection findings. Our Office assessed how the AFP was addressing this issue during our routine inspection in 2017–18 and again during a non-routine inspection conducted in 2018–19.'[113] The CO reported that educational activities were undertaken for the AFP. The CO does not report on exactly what happened to the AFP official or what action Parliament took to hold the AFP accountable.

In terms of section 180H, the AFP argued it only need to apply for a JIW if they need the 'metadata' of the journalist to help them identify the source. Given the quote of the CO above, it seems the AFP and the CO interpret section 180H differently. If they can identify the source with other information, they do not need to apply for the warrant. This means, the source may be identified without a warrant. A warrant is only required if identifying the source will be aided by the journalist's 'metadata'. The effect is that the AFP officials can identify the source without having to first obtain a JIW. The AFP can therefore bypass this requirement.[114]

The question is whether this was the intention of the protections that were worked into the law, or whether it is a gap in the law. If it is a gap, this gap may be exploited. The JIW process is therefore not effective, is poorly constructed and must be strengthened. If the intention is to identify the source, the AFP officials must in all instances first obtain a JIW. Not only should the 'metadata' of the journalist be protected by the JIW, as is currently the case, but also the 'metadata' of the source. In other words, even if the journalist's 'metadata' is not required to identify the source, but if the intention is to identify the source, the JIW must first be obtained in every situation. The JIW process should solely be based on the purpose of identifying the source and not on whether the journalist's data would aid the investigation of identifying the source.

To strengthen protections for whistleblowers, Section 180H can be re-written. Three options are proposed below. One, by inserting the underlined parts:

> *An authorised officer of an enforcement agency must not make an authorisation under section 178, 178A, 179 or 180 that would authorise the disclosure of information or documents:*
>
> *if the purpose of the authorisation is to investigate potential criminal offences or disciplinary conduct, under secrecy provisions in Commonwealth legislation or policies that prohibit the unauthorised handling of various kinds of information; and/or*
>
> *if the purpose of making the authorisation would be to identify <u>a journalist, a source of the journalist or an employer of the journalist</u>;*
>
> *unless a journalist information warrant is in force, and in relation to the said <u>journalist, employer or source.</u>*

Two, the section may alternatively be worded as follows:

> *An authorised officer of an enforcement agency must not make an authorisation under section 178, 178A, 179 or 180 that would authorise the disclosure of information or documents, if the purpose of the*

[112] The report can be accessed at: http://www.ombudsman.gov.au/__data/assets/pdf_file/0021/78123/CommonwealthOmbudsman-AFP-JIW-report-PDF-FOR-WEBSITE.pdf

[113] See footnote 102

[114] S Shanapinda 2018. PhD Thesis. (unpublished)

authorisation is to investigate potential criminal offences under secrecy provisions in Commonwealth legislation that prohibit the unauthorised handling of various kinds of information or if the purpose of making the authorisation would be to identify a journalist, a source of the journalist or an employer of the journalist;

unless a journalist information warrant is in force, in relation to the said journalist, employer or source.

Three, the section may alternatively be worded as follows:

An authorised officer of an enforcement agency must not make an authorisation under section 178, 178A, 179 or 180 that would authorise the disclosure of information or documents relating to a particular person if:

(a) the authorised officer knows or reasonably believes that particular person to be:

(i) a person who is working in a professional capacity as a journalist; or

(ii) an employer of such a person; or

(iii) a source of the said journalist or said employer; and

(b) a purpose of making the authorisation would be to identify the person whom the authorised officer knows or reasonably believes to be a source of the said journalist or said employer;

unless a journalist information warrant is in force, in relation to the said journalist, employer or source, under which authorised officers of the agency may make authorisations under that section.

These amendments will require the AFP to obtain a JIW in all instances where the aim is to identify the source: i). whether the AFP decides to use the journalist's 'metadata' to identify the source; or ii). whether the AFP uses other means, but still have the same aim of identifying the source. The AFP will not have the discretion to choose not to apply for JIW where it does not need the journalist's 'metadata'. Under this provision a JIW would always be required when violations of secrecy laws are investigated and when the source must be identified, irrespective of whether the 'metadata' of the journalists or the employer is needed for the investigation or not.

4.4 DEVELOPMENTS IN INTERNATIONAL JURISDICTIONS SINCE THE PASSAGE OF THE BILL

Since the passage of the Bill, courts in the UK and the US in 2018 responded to the statutory powers of the security and law enforcement agencies to collect and use telecommunications data by affirming the judiciary's oversight role – prior to the collection of the data. These international developments are critically discussed below, and in relation to Australia.

4.4.1 The *Carpenter SCOTUS* Case in the US about Location Information and Judicial Warrants Under the US Constitution

The *Carpenter* case took the fight over location information all the way to the Supreme Court of the United States (SCOTUS).[115] The case was about a series of robberies where no warrant based on probable cause was issued before investigators obtained the cell site location information. The location information was obtained based on 'reasonable grounds', with a believe that the information was relevant to an ongoing law enforcement investigation. The issue in the *Carpenter* case was whether the warrantless seizure and search of historical cell phone records that reveal the location and movements of a cell phone user for over 127 days was allowed by the Fourth Amendment.

Technology companies submitted a brief explaining:

- location tracking;[116]
- how the communications technology operates, by using smaller cells to reveal more precise locations;[117]
- how the telecommunications companies are used as one-stop shops by the law enforcement agencies to the extent that the agencies reduce the use of GPS tracking devices;[118]
- how a software market was developed to analyse location information on behalf of the agencies;[119]
- the personal nature of location information;[120]
- how the storage of location information by telecommunications companies are part of their ordinary business;[121] and
- the inherent nature of the telecommunications network to constantly transmit location information.[122]

Australian common law also contains the 'reasonable grounds' principle, as interpreted in the *George* case.[123] The facts the AFP will use to issue the authorisation and notification under the CAC Determination 2015 need to be sufficient to persuade the AFP that the collection of the location information is reasonably necessary or

---

[115] Timothy Ivory Carpenter v. United States (Supreme Court of the United States of America, No. 16-402, 28 September 2016) (14 August 2017) 13; S Shanapinda, 2018 (PhD Thesis, unpublished) pg. 178

[116] Technology Experts, 'Brief of Technology Experts as Amici Curiae in Support of Petitioner', Timothy Ivory Carpenter v. United States (Supreme Court of the United States of America, No. 16-402, 28 September 2016) (14 August 2017) 13.

[117] Ibid 15.

[118] Ibid 11. In Australia, in terms of 'Schedule 1—Australian Privacy Principles' and specifically 'Australian Privacy Principle 5—notification of the collection of personal information' in the *Privacy Act 1988* (Cth), the user must be informed if personal information is collected. In terms of 'Australian Privacy Principle 3.1— collection of solicited personal information', the Telco must only collect personal information if the information is reasonably necessary for or directly related to the Telco's functions. The Telco therefore collects all types of Location Information in the ordinary course of its business.

[119] *Carpenter* case

[120] Ibid 5.

[121] *Carpenter* case, pp. 6, 11.

[122] Ibid 9, 6.

[123] *George v Rockett* (1990) 170 CLR 104 20 June 1990 4 [8].

directly related to its functions or activities, as per the George case.[124] Despite the 'reasonable grounds' principle to collect the location information, and based on the constitutional right to privacy under the Fourth Amendment, on the 22nd of June 2018, the *Carpenter case* ruled that access to location information under the US' Stored Communications Act must generally be accompanied by a warrant issued under the probable cause standard, and not simply because the location information is reasonably necessary for an investigation and to enforce the criminal law.[125] In considering these developments after the data retention scheme was passed, Australia may need to increase the standard by which the Agencies collect and use location information, by similarly requiring a judicial warrant.

4.4.2 The Digital Rights Ireland Case and the Standard to Collect data When Strictly Necessary

The Directive 2006/24/EC[126] allowed for the retention and use of telecommunications data in the European Union (EU). The limit placed on this power was that such access must be necessary, appropriate and proportionate, within a democratic society for specific public order purposes. These purposes include: to safeguard national security, public security, the prevention, investigation, detection and prosecution of criminal offences.[127] Whereas the EU adopted the principle of 'necessity and proportionality' to protect privacy, Australia adopted the 'justifiable and proportionate' principle.[128]

Both the EU and Australia require that the collection of and the access to location information be proportionate to general public interest purposes. The key difference is that the EU standard requires necessity, a higher standard for the collection and use of location information considering that location information is crucial and that the EU agencies are not able to conduct investigations without it. The Australian standard requires the collection of location information to be justifiable. However, any activity collecting bulk location information may be justifiable for a wide range of law enforcement purposes, even if it has a discriminatory effect on minority groups. Directive 2006/24/EC allowed for the collection of a wide range of data from all types of communications. The *Digital Rights Ireland case* ruled that access to the telecommunications data, was in bulk, and therefore violated the right to privacy under the EU Charter of Fundamental Rights, even though the collection of location information was based on the higher 'necessity' standard.[129] In the EU, privacy must be protected at the higher standard – data may not be retained and accessed unless it is 'strictly necessary'.[130]

In Australia, as discussed in Part 4.1.5, under the exclusions, the Telco is only required to retain location information that is used to provide the communications service to the mobile device;[131] and only retain

---

[124] S Shanapinda, 2018 (PhD Thesis, unpublished)

[125] The *Carpenter case*.

[126] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[127] Articles 3 and 4 of Directive 2006/24/EC; Recital 4 in the preamble to Directive 2006/24.

[128] *TIA Act 1979* s 180F; *CAC Determination 2015*, Part 2 2.01 (1) Item 9.

[129] The *Digital Rights Ireland* case.

[130] Ibid [52], [56].

[131] *TIA Act 1979* s187AA (1) item 6.

location information at the start and at the end of a communication.[132] As discussed in Part 4.1.5, the exclusions to only store location information generated at the start and at the end of a communication, without a clear restriction not to store or collect location information prior to, during and after a communication, allows for the collection of more location information than is necessary. Despite the exclusions, revealing personal information may still be collected about the individual, that is more than necessary, but may be justifiable under this lower standard of 'justifiable and proportionate'.[133] This is so given the popularity of mobile communications and the frequency with which it is used by tech-savvy young people, as discussed in Part 4.1.7.

The use of Big Data (BD) analytics software may reveal more personal information about the individual and lead to misuse of the personal information collected. Another European Union (EU) protection is that EU legislation must lay down clear and precise rules governing the scope and application of the legislation.[134] The EU court decided that given the data will be processed automatically, there is a significant risk that the data may be collected unlawfully,[135] and it affects every persons communications, even the data of persons whose actions are not likely to be criminally serious[136] - in other words, there is no link required between the data required to be retained and the public safety that is being protected.[137] In Australia, under the exclusions, the location information of every persons' communications must be collected at the start and end; and may be collected voluntarily by the Telco, prior to, during and after the communication. The location information may be collected of persons not suspected of being involved in serious criminal activities to see if they may have been involved in serious and or non-serious activities and to then apply for warrants. Under this general rule, the location information of any person may be collected and assessed to see if at some point they committed a crime, and this would also be for public safety. Equally, the activities of young people planning climate change protests the Adani coal mine and the activities of the Greens, may potentially be assessed, without a judicial warrant, to see what plans they have of getting the Adani mine stopped, in the national economic interest. This general principle is therefore too broad in scope, to apply broad powers of the Agencies. There is therefore no specific, clear and precise link required between the location information required to be retained and the public safety objective. The only link required is that the collection of location information be 'in connection with'[138] the performance of the broad functions of ASIO,[139] or be reasonably necessary for or directly related to the broad functions and broad activities of the AFP.[140] Under these principles, collecting and inquiring into the activities of these political activist would be lawful, because the purpose is to enforce the broad functions and purposes of the activities, without clear and precise guidelines. Given the unclarity regarding the status of the Attorney-General's Guidelines and given how limited those guidelines are and that they allow for investigations even in cases where there is no violent protests, and the example of the FBI guidelines in the US, Australia may be in need of clear and precise public guidelines.

---

[132] Ibid ss 187A (1), 187AA (1) item 6.

[133] *TIA Act 1979* s 180F; *CAC Determination 2015*, Part 2 2.01 (1) Item 9.

[134] Digital Rights case [54].

[135] Ibid [55].

[136] Ibid [58].

[137] Ibid [59].

[138] *TIA Act 1979* ss 175(3), 176(3)

[139] Ibid ss 174(2), 175(3), 176(4)

[140] *Privacy Act 1988* (Cth) Schedule 1 Part 2 3.1, 3.4(d) (ii)

This is an indication of the broad discretion of the powers of the Agencies and how unlimited the access to and the use of location information is**.** Location information may be collected for minor offences and is not restricted to serious offences. As a result, there are no clear and precise rules have yet been publicly introduced in Australia governing the scope and application of the power to access and use location information. The limits imposed under the instruments such as the *TIA Act 1979,*[141] the *ASIO Act,* the *AFP Act,* the *Attorney-General's Guidelines* and the Ministerial Direction, do not outline a clear scope for the use of BD analytics software but supports the use of automatic means to process location information, and such projects have already been rolled out on the basis that collection of Open Source Intelligence (OSINT) location information, from social networks, are for the public good and safety.[142] Under these circumstances, Australia did not overcome the privacy challenges such as those faced by the EU when it introduced the 'justifiable and proportionate'[143] standard under section 180F of the *TIA Act 1979* and when it introduced the exclusions. These measures do not adequately protect privacy. Under the common law, privacy is generally protected as a by-product of other interest that are protected, such as confidentiality clauses from contracts with banks (Taylor 2000),[144] and privacy policies of the Telco and not under a Constitution containing a bill of human rights, as is contained under the Fourth Amendment in the US Constitution and the EU Charter. These contracts and privacy policies of the Telco's are set unilaterally by the Telco and skewed towards their commercial interests. As per the decision in the *Privacy Commissioner's case*,[145] for information to be regarded as personal, the individual must first and foremost be the subject of the information - a higher onus to bear.[146] Location information that is voluntarily retained and voluntarily disclosed to the Agencies, is not deemed to be personal, and must therefore first be about the individual, to qualify as personal information.

Australia ratified the *ICCPR* to protect privacy, but Australia's Constitution does not protect privacy. Under common law, privacy is only protected indirectly (Taylor 2000). Privacy is also protected under the *Privacy Act 1988* (Cth) and section 180F of the *TIA Act 1979* (Cth), which section introduced the principle of 'justifiable and proportionate',[147] but it does not adequately protect privacy the privacy of politically savvy and tech-savvy young Australians, for the reasons discussed earlier in Parts 4.1.5 to 4.2.2.

4.4.3 The Watson UK Case on Minor Offences and Data Retention

Under section 1 of the Data Retention and Investigatory Powers Act (*DRIPA*), the telecommunications company may be required to retain relevant communications data. The data may be retained based on the standard that the data is 'necessary and proportionate'. The retention notice issued, compelling the data retention, must describe the broad range of data and the period to be retained. The notice also covered

---

141 *Telecommunications (Interception and Access) Act 1979* (Cth)

142 Minister for Justice (Cth), Media Release, 15 June 2016

143 *TIA Act 1979* s 180F; *CAC Determination 2015*, Part 2 2.01 (1) Item 9

144 Taylor, "Why is there no Common Law Right of Privacy?", (2000) 26 *Monash University Law Review*

240-241; See: Loyd v Freshjeld (1826) 2 Car & P 325; 172 ER 147; Tournier v National Provincial & Union Bank of England [l9241 1 KB 461; Australia & New Zealand Bank v Ryan (1968) 88 WN (Pt I) (NSW) 368; Federal Commissioner of Taxation v Australia & New Zealand Banking Group (1979) 143 CLR 499; Barclays Bank v Taylor [l9891 1 WLR 1066; Winterton Constructions v Hambros (1992) 39 FCR 97, 114-15; Robertson v Canadian Imperial Bank of Commerce [l9941 1 WLR 1493; Christoj v Barclays Bank [2000] 1 WLR 937; Laster, 'Breaches of Confidence and of Privacy by Misuse of Confidential Information' (1989) 7 Otago Law Review 31,424

145 *Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 (19 January 2017)*

146 *Privacy Commissioner case* 15 [63]

147 *TIA Act 1979* s 180F; *CAC Determination 2015*, Part 2 2.01 (1) Item 9

historical and prospective data. The notice covered both serious and minor offences for purposes of national security, to prevent and detect crime, and in the interest of public safety.[148] The retained data could be disclosed under regulations or by a court order.[149]

The standards and the purposes for which location information may be collected in Australia, and the process appear to be similar to that of the UK. In Australia, an authorisation is issued to collect location information that is already retained.

In the *Watson* case, in January 2018, the UK Court of Appeal decided that if the retained data is used for minor offences, *DRIPA*[150] violates European Union (EU) law.[151] As a result, when it comes to preventing, investigating, detecting and prosecuting criminal offences, if the purpose for collecting and using the retained data is not limited to serious crime, Section 1 of *DRIPA* goes against EU law.[152] Instead, the retained data is collected in bulk and analysed using automated processing techniques, such as BD analytics software.[153]

DRIPA also violates EU law if the collection and use of the retained data was not pre-approved by a court or an independent administrative authority in review proceedings.[154]

The court declined to decide whether the individual should be informed after the retained data has been collected as *DRIPA* did not make provision for such a notification.[155]

EU law here refers to Article 8 of the *European Convention on Human Rights*, which protects respect for the individual's correspondence.[156] EU law also includes Articles 7 and 8 of the *EU Charter*, which protects respect for the individual's communication and the protection of personal data concerning the individual.[157] Australia has materially similar international obligations under the ICCPR.

4.4.4 Analysis of the EU, UK and Us Court Challenges

As represented by the court cases above and the relevant laws, the executive arms of all three US, UK and Australian governments appear intent on keeping the surveillance and investigatory power in the executive branch, shielded from judicial oversight. This is especially true with matters that relate to or are seen as posing threats national security. The Parts above discussed how the powers of law enforcement agencies have been challenged in the courts in the EU, the UK and the USA. A common theme is the negative effect of a lack of judicial participation in the process of collecting and using telecommunications data. Australia can be a leader in the field of privacy and introduce meaningful judicial participation when disclosing location information to the Agencies by introducing changes in its primary legislation. The legal challenge is based on

---

[148] *Regulation of Investigatory Powers Act 2000* (UK) cX, s 22(2)(a)-(h)

[149] *Data Retention and Investigatory Powers Act 2014* (UK) c X, s 1 (3), (6)(b)

[150] *Data Retention and Investigatory Powers Act 2014 (UK*)

[151] *Charter of Fundamental Rights of the European Union* [2000] OJ C (364/012000/C) Art 8–9; *Watson* case, 6, 3 [6.]; 6[13.]; 9 [27]

[152] *Watson* case 3 [6.]; 6 [13.]; 9 [27]

[153] Ibid 4 [6.2.e.1]

[154] Ibid 3 [6]; 6 [13]

[155] Ibid 7 [20] – [21]

[156] *Convention for the Protection of Human Rights and Fundamental Freedoms,* opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953)

[157] *Charter of Fundamental Rights of the European Union* [2000] OJ C (364/012000/C)

how revealing location information is technologically, and how severely this intrudes upon privacy protections contained in constitutional and international human rights charters. Legal challenges of this nature have not taken place in Australia, but the decision of the UK Appeals court declaring the law invalid due to judicial non-participation sends a strong signal that if democracies are serious about privacy protection, they should allow for prior administrative or judicial approval to the access and the use of telecommunications data, and not simply trust the judgment of the law enforcement agencies, as is the case in Australia. This seems to be the acceptable way the privacy of the individual may be legitimately interfered with in a democracy. Also, there must be clear guidelines to supervise the actions of the agencies.

4.4.4.1 The 'necessary and proportionate' Standard Did Not Adequately Protect Privacy In The UK

Australian law, (the amendments to the *TIA Act 1979* and the *TA 1997,*[158] that introduced the data retention scheme), is influenced by the EU's 2006 Data Retention Directive.[159] UK's *DRIPA* was based on the same 2006 Data Retention Directive.[160]

The *Watson* decision was made despite the 'necessary and proportionate' standard being part of *DRIPA*. In Australia, the privacy standards are 'reasonably necessary', 'on reasonable grounds' and 'justifiable and proportionate' (Selvadurai 2017)[161] and the 'in connection with' principle under the section 180F privacy tests.[162] The 'reasonably necessary' and 'justifiable and proportionate'[163] standards are lower standards than the 'necessary and proportionate' standard (Selvadurai 2017). The *Watson case* clearly illustrates that without prior judicial review to collect telecommunications data, privacy is not adequately protected. In those circumstances, the application of the 'necessary and proportionate' standard does not compensate for the lack of prior judicial approval and the use of the telecommunications data for minor offences. *DRIPA* and the EU Data Retention Directive 2006 can no longer be relied on as solid foundations for benchmarking after an ECJ critical review of the Directive in 2014. Australian law noted this and made changes in 2015. However, despite these positive changes aimed at strengthening privacy, privacy is still not adequately protected in Australia, compared to the UK, the EU and the USA. Selvadurai (2017) questioned whether the retention of telecommunications 'metadata' is a necessary national security initiative or a disproportionate interference with personal privacy, by analysing the Australian framework in relation to the ECJ's[164] decision, given the similarities between the two scenarios. Selvadurai (2017) described the data as valuable to the Agencies, referring to the benefit of identification of associations between communicators, providing a precise digital profile and matching the data with data obtained from social media, to identify persons of interest (Selvadurai 2017: 36). Selvadurai (2017) described the scope of the *TIA Act 1979*, to analyse the effectiveness in calibrating the privacy and national security interests (Selvadurai 2017). Selvadurai (2017) concluded the post-2015 Australian framework that allows for access to telecommunications data, was drafted in a manner that

---

158 *Telecommunications Act 1997* (Cth) *(TA 1997*)

159 Attorney-General's Department, 2014, 4 [A]. Note that the Directive was ruled invalid in 2014 by the ECJ

160 *DRIPA* Preamble

161 Niloufer Selvadurai, 'The retention of telecommunications metadata: A necessary national security initiative or a disproportionate interference with personal privacy?' (2017) 23(2) *Computer and Telecommunications Law Review* 35-41, 37; *TIA Act 1979* s 180F; CAC Determination 2015*,* Part 2 2.01 (1) Item 9)

162 *TIA Act 1979* ss 177(1), 178(3), 179(3), 180(4), 180F; *Privacy Act 1988* (Cth) Schedule 1 Part 2 s 3; *CAC Determination 2015*, Part 2 2.01 (1) Item 9

163 *TIA Act 1979* s 180F; *CAC Determination 2015* Part 2 2.01 (1) Item 9)

164 European Court of Justice

sought to overcome the privacy challenges the EU faced (Selvadurai 2017: 35- 41). Selvadurai (2017) referred to the EU Data Retention Directive[165] that was invalidated by the Court of Justice, stating that, given this legal precedent, it is interesting that Australia requires the retention of specific kinds of telecommunications data (Selvadurai 2017: 36). Australian courts on the other hand, endorsed the 'in connection with' principle and the 'reasonable grounds' principle in the *Samsonidis,*[166] *Gant*[167] and *George*[168] *court* cases, where warrants were issued by a judicial officer or an administrative body. It would be interesting to see how an Australian court would rule on these standards where no prior judicial oversight took place, as in the *Watson* case. In this submission I assessed whether the Australian location information retention and disclosure framework can really be said to have overcome the privacy challenges. Part 4 as a whole, and specifically Part 4.4, has raised the privacy oversight challenges that remain, specifically under the 'justifiable and proportionate' principle, in combination with the 'in connection with' principle and the 'reasonable grounds' principle. This is so despite the privacy safeguards introduced in 2015. This situation is generally contrary to the claim by Selvadurai (2017) that the post-2015 Australian framework was drafted in a manner that sought to overcome the privacy challenges the EU faced (Selvadurai 2017). The Australian framework may therefore require a judicial warrant system to fully overcome the privacy challenges that still exist.

4.4.4.2 Australia can be a Human Rights Leader

In the USA, the EU and the UK the legal challenges to the collection and use of location information are based on the Constitution and international human rights charters. While there is no equivalent constitutional protection in Australia, Australia is a signatory of the *ICCPR* that protects privacy under Article 7. The Parliamentary Joint Committee on Human Rights (PJCHR) uses Article 7 as a measure for Australian law.[169] The study could not locate an Australian court case where the access and use of location information has been challenged on the basis that location information is used for non-serious offences and was not pre-approved by an independent judicial or quasi-judicial body.

In the US and the UK, the *Watson* and *Carpenter* cases challenged the law, accusing it of not balancing privacy proportionately and not using a higher standard to access location information. The *Watson* case is setting a precedent for a UK ally such as Australia whose laws have similarly excluded prior judicial review of the notices and authorisations under the *CAC Determination 2015* to collect and use location information for law enforcement and security purposes. Access to retained data may possibly be challenged in Australia under the same principles as in the UK and the USA, but on legal grounds that are unique to Australia, as described in this book. These principles include:

- the lack of independent judicial oversight, the use of the location information for non-serious offences and the bulk collection of the data – when compared to the UK; and

[165] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[166] *Samsonidis v Commissioner, Australian Federal Police* [2007] FCAFC 159 (5 October 2007)

[167] *Gant v Commissioner Australian Federal Police* [2006] FCA 1475, 12 [42]

[168] *George v Rockett* (1990) 170 CLR 104 20 June 1990 4 [8]

[169] PJCHR, Human rights scrutiny report Thirty-fifth report of the 44th Parliament (25 February 2016), 18, 25 [2.48]

- the use of the low standard of the location information being reasonably necessary for broad policing functions to collect the location information, as opposed to being based on a higher standard equivalent to probable cause or reasonable suspicion – when compared to the USA.

In all instances, the common thread is that the challenges are based on requiring a higher standard and independent oversight to access data that is considered to be personal in nature and over which individuals have a right to privacy under their Constitutions, unlike in Australia. Australia however has no direct common law right to privacy, and no bill of rights in its Constitution for the protection of privacy under the Australian Constitution, whereas in the EU there is a Charter of Rights.

As UK laws were impacted by the *Watson* decision, notwithstanding that Part 4 of *DRIPA* is under review, the *Watson* decision sends a strong signal that pre-reviews of the access to retained data should be a basic measure of privacy protection. The review of Part 4 of *DRIPA* will have to consider the *Watson* decision. The challenges indicate that the tide may be turning against the privilege of the executive branch of government to make the sole decision on accessing telecommunications data. It is advisable for Australia to look into the future and introduce a location information warrant regime as proposed below, without first having to resort to a court challenge, unlike its allies. If Australia continues to maintain its current retention and disclosure framework after the *Watson* and *Carpenter* cases, from a judicial perspective, Australia may be isolating itself from two major jurisdictions with which it is allied. The time is right for the Australian Parliament to become a leader in human rights. As stated above, privacy is generally protected as a by-product of other interest that are protected, such as confidentiality clauses from contracts (Taylor 2002).[170] Customers of the Telco are protected by privacy policies and standard terms and condition that contain clauses to protect the privacy of the customers, and under the *Privacy Act 1988*, subject to the exceptions that apply to the benefit of the Agencies.[171] Given that Australia does not have a common law privacy right that directly protects privacy but only does so indirectly, in this submission I humbly propose that Parliament amend the *TIA Act 1979* to require judicial review of the authorisations and notifications prior to the collection and use of location information. Continuing the status quo places Australia, as a democracy, under a very peculiar position globally – location information may be collected and used for law enforcement and security without any prior judicial review and under a very low standard of the location information only having to be necessary for policing and broad security purposes. In the UK, regarding the issue of law enforcement, this legal position would be a violation of privacy, as a human right, a right that Australians may not be able to directly claim under their Constitution. The *Privacy Act 1988* and the *TIA Act 1979* in section 180F protect privacy, but subject to the superior powers of the Agencies to collect personal information for broad law enforcement purposes, and without prior judicial review. Comparably, Australia's position cannot be said to be proportionate, given that the location information collected may be used without judicial involvement and for non-serious offences, given the sensitive information location information may disclose with the use of BD analytics software. Australia's poor privacy protection position is comparably at odds with the *EU Charter* and generally with human rights in the EU and the USA.

---

[170] See Loyd v Freshjeld (1826) 2 Car & P 325; 172 ER 147; Tournier v National Provincial & Union Bank of England [l9241 1 KB 461; Australia & New Zealand Bank v Ryan (1968) 88 WN (Pt I) (NSW) 368; Federal Commissioner of Taxation v Australia & New Zealand Banking Group (1979) 143 CLR 499; Barclays Bank v Taylor [l9891 1 WLR 1066; Winterton Constructions v Hambros (1992) 39 FCR 97, 114-15; Robertson v Canadian Imperial Bank of Commerce [l9941 1 WLR 1493; Christoj v Barclays Bank [2000] 1 WLR 937; Laster, 'Breaches of Confidence and of Privacy by Misuse of Confidential Information' (1989) 7 Otago Law Review 31,424

[171] Vodafone Hutchinson Australia, *Privacy*, 2017

In its submission on the Data Retention Bill, the AGD stated that Australia would be violating its international obligations under the Budapest Cybercrime Convention, if Australian law were to limit access to historical 'metadata' to only serious crimes.[172] In other words, to meet its international obligations, Australia must allow access to historical 'metadata' for non-serious offences as well. As highlighted by the UK and US court decisions, the trend amongst Australia's allies is that, as far as the judiciary is concerned, international rights and constitutional rights require that access to historical 'metadata' must only be accessed with a judicial warrant. If Australia amends the *Data Retention Act 2015* (Cth), requiring a judicial warrant to access location information and other 'metadata', then Australia would be complying with its international human rights obligations. Not doing so, may be a failure of Australia's international human rights obligations under the ICCPR. Article 17 requires that Australia protect the right to privacy. The international trend seems to be that privacy is best protected, in a democratic society, if a judicial warrant is required to access location information and other 'metadata'.

The Australian legal framework to collect and use location information may generally be described as follows:

i. it is a process of self-certification and there is no prior judicial oversight required to access the location information;[173]

ii. the location information is used for all types of offences, for broad inquiry and investigatory powers;[174]

iii. there is little chance to challenge the powers of the Agencies even after the collection of the location information, given the confidential nature of security investigations;

iv. the *ex post facto* oversight is done by bodies that are under the control and are part of the executive arm of government;

v. there is bulk collection and use of very revealing and personal BD, able to be used in machine learning software;

vi. the location information may be used for any law enforcement and security activities which may be possible to justify as reasonably necessary to enforce the law and to protect the national security of Australia, despite the political biases and motivations, although this is not known to have taken place; and

vii. for Australia, the legal issue essentially comes down to whether the current legal framework, under these circumstances, can be said to fairly and adequately advance privacy protection. A judicial warrant process may better protect privacy, as proposed below.

The framework may be improved with the recommendations discussed below.

---

[172] AGD. 2015 submission to the PJCIS Inquiry into the Telecommunication (Interception and Access) Amendment (Data Retention) Bill 2014, page 44

[173] Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 30 January 2015, 31 (Peter Leonard Guildford, Chairperson of the Media and Communications Committee, Business Law Section of the Law Council of Australia)

[174] Attorney-General's Guidelines s 6.1; *AFP Act 1979* (Cth) ss 4(1) (definition of 'police services'), 8(1) (bf)(ii), *Telecommunications (Interception and Access) Act 1979* (Cth) (*TIA Act 1979*) s 181

5. Recommendations

This section proposes stricter procedures and requirements to access and use location information by means of a Location Information Warrant (LIW). It is recommended that the *TIA Act 1979* be amended to incorporate the LIW, and other suggestions made below.

5.1 THE LOCATION INFORMATION WARRANT - PROPOSED PROCEDURE

The authorisation and notification under the *CAC Determination 2015* can be described as a 'self-certification process'[175] that is supported by a low threshold,[176] to use location information for the wide investigatory powers of the Agencies.[177] The LIW process will encourage greater public trust and confidence if independent oversight bodies assess and pre-approve the applications for location information. It is crucial that the impact on the privacy of the individual (or group of vulnerable individuals such as the tech-savvy young people) and the proper level of restraint appropriate, is assessed in advance, by an independent third party. This independent third party should be sufficiently independent from the AGD, ASIO, ASD and the AFP. Bureaucratic hurdles that may be created by these changes are also addressed in Part 5.5.5.

5.1.1 The Types of Location Information that are Legally Personal Information

The better means of protecting privacy is to state clearly in the *TIA Act 1979* and the *Privacy Act 1988* that location information is personal information, as a matter of law (as is already done on a narrower basis in section 187LA of the *TIA Act 1979*). Location information that is personal information should include, and be described as:

i. the velocity, altitude, latitude about a mobile telecommunications device and the identity of a base station (cell tower);

ii. whether a data point is accurate or estimated;

iii. whether it is used for billing or not; and

iv. whether generated prior to, at the start, during, at the end of, or after a telecommunications service; and

v. when linked with other information,

that is able to identify an individual and reveal personal information about the individual, whether aided by or not, the use of data analytics software.

---

[175] Evidence to PJCIS (Peter Leonard), 2015

[176] Evidence to PJCIS (Thom), 2015

[177] *TIA Act 1979* ss *174* (2), 175 (3), 176(4)

Before collecting location information from the Telco, the Agencies should be required to obtain a LIW, after which the location information may be used. The LIW should be required even if no person is named, or no IMSI, account number or phone number is used to request the location information. Under these circumstances the LIW is a better protection for the privacy of the individual.

5.1.2 The Authority to Whom the Application Should Be Made

To strike an acceptable balance between the powers of the Agencies, public safety interests and privacy interests, and to minimise the conflict of these interests, an independent authority must be appointed to receive applications for a LIW. The independent third party could be: i.) a quasi-judicial body, with sufficient independence; and/or ii.) a court overseen by a Judge or magistrate, as an independent member of the judiciary – independent from the executive branch of government, but with a security clearance. The independent party would dilute the concentration of power in the hands of the AGD and the Minister of Home Affairs, and the Agencies. The third party would ensure predictability in the process, for the Telco to disclose more location information. The proposed balanced requirements and procedures are described below.

5.5.3 Exceptions to Making the Application

One must be mindful to avoid undermining the critical role of the Agencies and causing unnecessary delays to investigations. The Agencies would not be required to make applications for the LIW under the following circumstances:

If the time it will take to apply for the LIW, obtain the LIW and thereafter obtain the location information from the Telco would involve unreasonable delays that severely compromise or severely impede the investigation, inquiry or enforcement of the criminal law where time is of the essence. A severe compromise may be caused if the individual is very likely to escape while approval of the LIW and the collection of the LI are pending, making it very difficult or impossible to locate the individual or identify the individual. A severe impediment may be caused if the location information collected after the LIW is issued may not be useful or relevant any longer.

If it would cause a severe compromise which is unable to be remedied after the LIW has been collected.

Despite the above exceptions, the issuing authority must in any event be informed of the following, at all relevant times when access to location information is required, and be given copies of records within a reasonable time after issuing an authorisation and notification to the Telco to collect the location information:

i. The justification, based on reasonable grounds and in good faith, for seeking to avoid having to apply for the LIW, if the Agencies seek this. The reasons may include that applying for the LIW may cause unreasonable delays that may compromise the investigation, the inquiry or the enforcement of the criminal law.

ii. A copy of the authorisation and notification issued to the Telco, stating specifically that the officer considered the facts at hand; outline the facts; how he or she applied the 'Privacy Tests' and the 'Reasonably Necessary or Directly Related Tests' to the facts; the reasons for and against issuing the authorisation; and why the authorisation was approved to be issued and why it could not be denied.

iii. The location information collected from the Telco.

iv. The records kept that relate to the authorisation and notification.

5.5.4 The Role of the Authority

The approving authority may study the authorisation and retrospectively validate the authorisation, and impose any restrictions, prior to the collection of the location information. If the location information was already collected the approving authority may direct how privacy risks identified may be minimised going forward.

The Agencies and the Telco must keep the approving authority updated about how the location information was used, how BD analytics software analysis was used, how useful it was or not, how privacy risks were minimised, and if the authorisation needs to be renewed, the reasons for such renewal.

5.5.5 The Procedure to Request Location Information

The existing procedures used for warrants, investigations, the *CAC Determination 2015* and the Attorney-General's Guidelines[178] would be strengthened by implementing the following recommendations:

i. In the event the Agencies or the Telco apply for a LIW, the Agencies may inform the Telco and the Telco may inform the relevant agency of the application. The other party can be informed of the details of the LIW intended to be disclosed, and the reasons, based on reasonable grounds and in good faith. The notice can request the other party to take any preparatory action while the application is being processed. In this manner any time delays may be minimised. The preparatory action would relate to any action the other party would be approved to take under the LIW. The Telco may start the initial process of gathering the LI, so as to be able to disclose the location information once the LIW is approved and issued to the Telco;

ii. The LIW warrant may be applied for on an *ex parte* basis by the Agencies or the Telco;

iii. The issuing authority of the LIW must assess and be satisfied that the Agencies only collected location information that was reasonably necessary, on reasonable grounds, in good faith, and that the disclosure or use was justifiable and proportionate, based on the gravity of the offence and related matters, and that the LI was relevant and useful;

iv. The Agencies should specify the facts, the allegations under investigation or matter being inquired into, the law enforcement and security activities of the Agencies, on suspicion of a past, present or future offence, based on reasonable grounds;

v. The Agencies should clearly set out reasons to the issuing authority, based on the relevant circumstances, why the person should not be informed of the collection and the use of the location information. There may be circumstances that justifies that the person is informed. For example, it may be in the interest of national security if a person is being recruited by a foreign government, to

[178] Attorney-General's Guidelines, 2016.

warn the person of such efforts, so as not to cooperate. If informing the person would prejudice security and compromise law enforcement investigations, not informing the person may be justified;

vi. The Agencies should clearly set out reasons to the issuing authority, based on the relevant circumstances, why the person should not be given copies of the authorisation and notification issued under the *CAC Determination 2015* to collect and use the LI and should not be allowed to challenge the collection and use of the location information;

vii. The reasons for the application of the authorisation and reasons why it should not be denied, based on reasonable suspicion and belief, under oath or affirmation;

viii. The likely relevance and usefulness of the location information to the investigation, inquiry and the law enforcement and security activities directly or indirectly related to the functions and purposes of the Agencies;

ix. The issuing authority may request further information;

x. The issuing authority may grant or refuse to grant the application for the LIW in full, or partially grant or partially refuse the application for the LIW;

xi. A reasoned statement by the issuing authority, based on the supporting documents submitted, outlining the reasons for the decision;

xii. The reasons for the decision should state the privacy risks identified and how those risks were mitigated; and

xiii. The decision by the issuing authority should state relevant restrictions regarding the collection and use of the location information.

5.5.6 The Types of Location Information Requested to be Disclosed

Under the LIW, the following types of location information may be requested and be approved to be disclosed by the independent authority:

i. The location information used to deliver the Short Message Service (SMS) or voice communication to the mobile device;[179]

ii. The location information not used to deliver the SMS or voice communication to the mobile device, in other words, the neighbouring or Enhanced cell-ID (E-CID);[180]

iii. The location information generated prior to, during, at the end of and after a voice or SMS communication;

[179] *TIA Act 1979* s 187AA (1) item 6.

[180] Revised Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Cth), 2015, 44 [246].

iv. The location information generated when the individual is not using the device, also referred to as pings and regular connections that mobile devices make to cell towers;[181]

v. The location information stored by the Telco for any period, for commercial and for purposes to maintain the telecommunications network, if the Telco has the location information in its possession;[182] and

vi. The IMSI and IMEI of the mobile device, and similar device-type identifiers that may be in use.

5.5.7 The Standards to Safeguard Privacy

The 6 standards discussed below are proposed to be incorporated into the LIW to strengthen privacy protection. Section 180H may need to be re-worded, as recommended in Part 4.3.1.

5.5.7.1 Transferring Guideline 10.4 and Guideline 13 to the LIW

Firstly, it is recommended that the existing privacy protections included in the Attorney-General's Guidelines be transferred to the LIW,[183] so that it has the force and effect of a legislative instrument and minimises the discretionary powers of ASIO. The Attorney-General's Guidelines should be updated to address how ASIO must address situations where sensitive information such as political affiliations and ideologies, regarding climate change and projects that impact the environment and conflict with national economic interests, including how they are to be resolved and how ASIO must prevent political influence from the executive branch of the government and staff members in the various government departments.

5.5.7.2 Transferring the privacy standards from section 180F of the TIA Act1979 to the LIW

The privacy protections under section 180F[184] should be applied to ASIO under the LIW. The AAT member, the Judge or magistrate should be satisfied that the privacy test justifies the collection and use of the location information.

5.5.7.3 Guidelines for methods considered intrusive and methods considered less intrusive

The LIW should require the Agencies to '… clearly document whether less intrusive methods have been considered and explain if they are not likely to be effective in a particular case'.[185] ASIO is required to use less intrusive techniques if feasible.[186] To access and use location information, clear guidelines should be developed distinguishing between what is considered less intrusive in accessing and using historical location information versus the level of intrusion from using prospective location information. In the interest of public trust and transparency, these guidelines should be made public.

---

[181] Ibid.

[182] *TA 1997* s 275A, 276, 280, 313(3), 313(4), 313(7); *TIA Act 1979* ss 175–184.

[183] Attorney-General's Guidelines ss 10.4, 13.

[184] *TIA Act 1979*

[185] OIGIS, 'Annual Report 2014–2015', (2015), 2425

[186] Attorney-General's Guidelines s 10.4(b)

5.5.7.4 Guidelines for Activities That May be of Interest to National Security

The United States has guidelines on racketeering and domestic terrorism offences.[187] These are the 'Attorney General's Guidelines On General Crimes, Racketeering Enterprise And Domestic Security/Terrorism Investigations' for the Federal Bureau of Investigations (FBI) and they are public.[188] Australia should have similar guidelines. The AGs' Guidelines and the AFPs' Ministerial Guidelines should be amended, to clear distinguish between activities that would qualify as threats to the national security and economic interests, vis-à-vis political activities that are acceptable in a democratic society. Overlaps should be addressed, and the criteria should clearly state how the one overrules/trumps the other, the reasons for it and how such a decision can be challenged. The guidelines should clearly outline how these types of sensitive activities will be referred by any member of the Executive to ASIO, AFP and ASD, for an inquiry, investigation, law enforcement or national security assessment, and how such matters should be handled. The guidelines should be contained in a legislative instrument. The independent judiciary should be granted powers to inquire into the operational activities and those affected should be allowed access to the evidence that will be used against them to challenge the collection and use of 'metadata' from inception and when presenting charges in court.

Introduce clear guidelines and restrictions about the conflict between national security and political activity by young people and political parties, when it comes to climate change and mining activities that may negatively impact the environment but have great economic promise.

The role and applicability of the Attorney-General's Guidelines, in relation to the collection and use of location information and other 'metadata' by ASIO and the AFP should be clarified.

5.5.7.5 Review of the LIW

Currently the individual is not able to see the location information collected about them. The individual should be allowed to access the LIW. The individual should be allowed to challenge the disclosure of the location information, under the LIW, by means of judicial, quasi-judicial review (administrative review) and freedom of information disclosure procedures. Any objections to a request should be subject to an administrative challenge and review by the courts.

5.5.8 The Oversight Roles of the OIGIS and the Commonwealth Ombudsman

If the privacy standards cannot be met by the Agencies, the oversight bodies should report on the extent it was met or not, and the reasons and specific recommendations in each case. The oversight bodies should make specific recommendations of changes to be made to the laws and the legislative instruments, as part of their annual reporting.

5.5.9 Creating a Feedback Loop

The full report of the OIGIS and the Commonwealth Ombudsman, with classified details, should be submitted to the Judge or magistrate with a security clearance that issued the LIW. The issuing authority must consider

[187] Department of Justice, Attorney General's Guidelines On General Crimes, Racketeering Enterprise And Domestic Security/Terrorism Investigations (2 March 2017). https://www.justice.gov/archives/ag/attorney-generals-guidelines-general-crimes-racketeeringenterprise-and-domestic

[188] Department of Justice, 2 March 2017

the report and issue a separate report to the Agencies, the Commonwealth Ombudsman, the OIGIS, the AG, the Prime Minister and the Parliamentary Joint Committee on Intelligence and Security (PJCIS), with recommendations. In this manner there is a full feedback loop that all relevant and interested authorities have insight into the exercise of the powers and the information is shared, transparently and are less reliant on boilerplate non-specific formal statements, and in this manner, privacy is better protected, and risks of excessive intrusion are minimised.

5.5.10 The Journalist Information Warrant

The Agencies are not clear on when to apply for a Journalist Information Warrant (JIW). The JIW should include as a sub-category under the LIW. The sub-category should clarify that whenever any matter where the location information of a journalist, the employer of the journalist, or the source of the journalist is to be collected for an inquiry, investigation, to enforce the criminal law, to perform an activity related to the functions and purposes, or an activity related to performing their functions and purposes, the LIW should be applied for.

The alternative proposal is contained in Part 4.3.1.

5.5.11 Reporting Statistics

In the interest of transparency, the statistics should specifically indicate the disclosure of location information whether disclosed under an authorisation or voluntarily by the Telco, in respect of both Agencies, and any other body that may be obtaining access.

5.5.12 Amendments to the TIA Act 1979 and the TA 1997

The necessary amendments need to be made to the *TIA Act 1979,* the *Privacy Act 1988,* the *TA 1997,* the *CAC Determination 2015*, the Attorney-General's Guidelines and the Ministerial Guidelines to cater for the above changes.

6. Conclusion

This submission highlighted that recent developments in location precision communication technologies puts young Australians also referred to as 'digital natives', and who are tech-savvy, environmentally-woke and politically savvy; and whistle-blowers, potentially most at risk of being surveilled under Australia's unique location data retention and disclosure scheme. The justification will be 'security', but 'security' is so broad that it can be misused. The submission therefore proposed a judicial warrant to collect and use location information. This change is necessitated given the location precision 5G technology will provide, for vehicular traffic, mobile phones and people, basically acting like ankle monitors, but that are instead carried in bags and handheld. This positive change will put Australia on par with its western allies.