TelSoc
Telecommunications & the Digital Economy
Published on *Telsoc* (https://telsoc.org)

Privacy of Location Information

Stanley Shanapinda [1]

University of New South Wales

AJTDE - Vol 6, No 4 - November 2018 [2]

[3]

☆ 103[4]

Abstract

This article reviews existing knowledge regarding the powers of the Australian Security Intelligence Organisation and the Australian Federal Police to access and use metadata. The review is primarily based on published research on the privacy impact of the revised metadata retention and collection framework introduced in 2015. The review reveals that, after 2015, no comprehensive study was undertaken in the following areas: how location information is generated and exchanged in the IP-mediated long-term evolution telecommunications network, and how mobile devices are tracked and create more precise location estimates, in the legal and policy context of the exceptions and privacy safeguards introduced after 2015; the discretionary powers of the agencies to use personal and sensitive information to identify inquiries and investigations to pursue, to enforce the law and perform their functions, and to carry out activities related to their functions and purposes; and the flexible oversight principles contained in the guidelines that create conflicts between law enforcement and privacy interests. The review proposes future multidisciplinary research.

Introduction

The retention and disclosure of metadata to law enforcement agencies has been met with criticism worldwide and has been invalidated by the courts. The broad range of investigatory powers are not regarded as being consistent with the protection of privacy (*the Watson case* [5], 70; *Digital Rights Ireland Ltd, 2014* [6], [60]*; USA FREEDOM Act* [7]; *Carpenter case, 2018* [8]).[i] [9] This review highlights arguments that state privacy is not adequately protected, given the investigatory powers of the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP) (the Agencies) that appear broad and based on how Location Information (LI) is personal and precise, given the use of modern telecommunications technologies. The review raises complex issues that at times appear to be at odds with one another. This complexity highlights the need for in-depth studies, in the interest of a nuanced privacy debate. This review highlights these arguments in relation to existing literature and states that existing literature did not adequately study the contemporary powers of the Agencies to collect retained data in relation to how modern communications technology generates and shares LI and the personal nature of LI. As such, an empirical study must still be undertaken. The proposed study is likely to confirm that privacy is poorly protected, but the benefit of such a study would be the relevant findings that are based on current contexts about how the powers of the Agencies are designed and operate.

The issues raised by other authors included: understanding how modern mobile phone location services work to balance the powers of the Agencies; the privacy characteristics of telephone metadata in America; inadequate protection of privacy; the lack of transparency in the exercise of the powers of the Agencies; the broad powers of the Agencies and whether telecommunications data is considered âpersonal informationâ; and the impact on privacy by the use of Big Location Data (BLD) analytics software by the Agencies for investigations. Criticism of the powers of the Agencies were made through the privacy lens â i.e. the focus was largely on the impact of the powers on privacy. Whereas the impact of the powers of the Agencies on privacy is not a new issue, this review also approaches privacy from the perspective of privacy being a tool that is used to restrict the powers of the Agencies. There is a difference between how privacy was protected in 1988 when the *Privacy Act* [10] was introduced, and how privacy is protected since 2015, when the *Data Retention Act 2015* (Cth) [11] introduced the two-year mandatory retention of LI. There is no comprehensive study of the privacy safeguards revised in 2015, both as principles to be protected and as limits to the powers of the Agencies and how privacy is impacted by the very powers it aims to restrict. This review recommends empirical studies based on how privacy can be used to exercise oversight over the powers of the Agencies. Studies must look at this dynamic interaction to understand how privacy is impacted but also how privacy plays the role of gatekeeper. Privacy is not a static standard, it evolves with time, and has a dual nature â as a target and as an oversight tool. The LI generated by new communications technologies such as LTE (the mobile fourth-generation long-term evolution standard) is more revealing of Personal Information (PI) and Sensitive Information (SI), and so the definition of what is considered âpersonal informationâ changes with time. This review raises relevant and modern issues that provide the context needed to try to understand the modern privacy debate. The review makes a preliminary conclusion that the use of modern communications technologies leaves privacy more vulnerable than before, when earlier authors wrote about the impact on privacy. To strike a fair balance between privacy as a right to be protected and simultaneously using privacy as a tool to limit the powers of the Agencies, privacy may require greater protection than before. The requirement to retain the information for a minimum period of two years, or longer, creates an incentive for the Telco to collect and store more LI than the Telco ordinarily stored, and for use in new commerce developing digital products and digital services (AGD, Submission 2015 [12], 16â17 [2.3]; Telstra, Submission 2015 [13], 5 [8]). The same LI may in practice be retained for longer than the two-year minimum and remain available to the Agencies without a judicial warrant throughout its lifespan (*TIA Act 1979* [14] ss 5(1) (definition of âretained dataâ), 187C, 175â184; *TA 1997* [15] ss 275A, 276, 313(3), 313(4), 3131(7)). This weakens the position of privacy as a principle to be protected and as a safeguard for the accountable exercise of power, in the context of BLD.

Existing common law precedents must be analysed in detail in the context of the 2015 data retention scheme. These include:

- The 2015 *Telstra Corporation Limited* case [16] ([2015] AATA 991 (18 December 2015)) and the 2017 *Privacy Commissioner* case [17] ([2017] FCAFC 4 (19 January 2017)), where the meaning of PI was argued â whether the data in question can be about multiple things, including being about the individual or not;
- The *Farrell* [18] ([2017] AATA 409 (31 March 2017)) case and the *Jaffarie* [19] case, where the broad meaning of national âsecurityâ was contested but accepted by the courts;
- The *Day* [20] ([2000] FCA 1272 (11 September 2000)) case where the court decided that the word âinvestigationâ is taken to mean âthe act or process of searching or enquiring in order to ascertain factsâ. This case was not critically analysed in relation to the use of BLD analytics and the resulting impact on privacy; and
- The *Samsonidis* [21] case ([2007] FCAFC 159 (5 October 2007)) that effectively makes the point: if the information collected for the purpose of investigation A was shared within one organisation to perform investigation B, the organisation would be allowed to do so, without having to apply the privacy tests in respect of investigation B before sharing the data. The *Samsonidis* [21] case needs to be critically analysed in relation to the privacy impact of its interpretation when it comes to the use of BLD analytics, that reveal more SI and PI, about peopleâs behaviour that may not be related to the investigation in question and in relation to third parties that may not be primary targets of investigations.

The sections below review key issues raised in existing literature related to the collection and the use of metadata, in relation to its impact on privacy.

Understanding How Modern Mobile Phone Location Services Work to Balance the Powers of the Agencies

Leonard (2015c [22], p. 7) suggested that an understanding of the types of data that will be collected, and the entity collecting the data, could help assess the effectiveness of any limits that are placed on receiving the telecommunications data. Location Information is identified as one such data type and is the focus of this review, in order to try and assess the effectiveness of any limits on collecting and using LI. The review distinguishes between the two Agencies, assessing their powers individually. Leonard (2015c [22], p. 7) also stated Australian telecommunications law that deals with the disclosure of information regarding communications is vague and does not address modern issues. An LTE mobile telecommunications network (ETSI 2017a [23]), with its more precise location functionality, is one such modern technological issue and is raised as the focus of this review.

Taking a historical look, Leonard (2015c [22], p. 7) made the point that the ambiguity in the law can be traced back to the reason why telecommunications interception was developed. The reason was to protect privacy of voice telephone calls. The calls were mediated by copper wires (Leonard, 2015c [22], p. 7). The information about communications using copper wires was deemed less sensitive than the contents of the phone call (Leonard, 2015c [22], p. 7). This distinction between the voice call (as the contents of the communication) versus the time and duration of the call (as the information related to the voice phone call) is now the basis of Australian telecommunications interception law (Leonard, 2015c [22], p. 7). American electronic surveillance legislation has also drawn distinctions in protection between the content of a communication and information that is related to the content of a communication. This was at a time when content and metadata were more distinct (Bellovin_2016 [24], pp. 2, 3, 8, 17).

Information about communications is accessed by the Agencies under the less stringent *CAC Determination 2015* [25] because the metadata is considered less sensitive than the content of SMS or voice messages (*TIA Act 1979* ss 174 â 84 [14]; *TA Act 1997* s 275A [15]). Bloch and Wark (2015 [26]) cited the recommendation of the Parliamentary Joint Committee on Human Rights (PJCHR) that âcontentâ be defined, in order to better protect privacy (Bloch & Wark, 2015 [26], pp. 23-27). The report, however, did not go to the extent of recommending an actual definition for the type of information that should be considered âcontentâ. The critical question to be examined is how the distinction between content and metadata is relevant to the discussion regarding the protection of privacy, given the modern Internet-Protocol (IP)-mediated LTE network. In an advanced IP-mediated, LTE mobile network, from a technological perspective, the lines between metadata and content are blurred, as discussed below. In the IP-mediated LTE network, LI is created, exchanged, and stored in a Stream Control Transmission Protocol/Internet Protocol (SCTP/IP) packet over the Internet, which is technologically speaking, a communication (IETF, 2007 [27], 6 [1.2], 15 [3]; ETSI, 2017a [23], 22 [6.4.1-1]). The network architecture is illustrated in Figures 1 and 2. Figure 1 is best read from left to right to understand how the various pieces of equipment in the IP-mediated LTE network operate. Location Information is carried as the LTE Positioning Protocol Annex (LPPa) message inside the S1 Application Protocol (S1AP) message, as its content, between the two devices, such as the Evolved Universal Terrestrial Access Network (E-UTRAN) Node B (eNB) in the EUTRAN and the Mobility Management Entity (MME) (ETSI, 2017d [28], 7 [1], 10 [6]; ETSI, 2017e [29], 91 [8.17.1], 92 [8.17.2.1-1]). These messages include Assistance Data, Measurements and LI forwarded from the User Equipment (UE), which is the mobile device, and the MME by using the LTE Positioning Protocol (LPP) (ETSI, 2017a [23], 21 [6.2.1]). These Network Elements work together by exchanging radio signals and the identity of the UE, to help locate the position of the UE and to store the location of the UE (ETSI, 2016a [30], 145). The connections between these Network Elements are made over the Internet (ETSI, 2017a [23], 91 [8.17.1]). The Network Elements use various interfaces and Internet-based protocols to exchange these messages (ETSI, 2017f [31], 24 [4.1.1.1]).

[32]

Figure 1. The IP-mediated LTE Network (ETSI, 2017f [31], 58 [5.2.3])**[ii]** [33]

Location Information is technologically, from the perspective of the IP-mediated LTE network, carried inside an Internet Protocol (IP) packet, as the contents of the IP packet. The LPPa signal messages are communication(s) carried over the Internet by means of these various protocols, such as the SCTP/IP (ETSI, 2017a [23], 21 [6.2.1]; Kozierok, 2005 [34]; IETF, 1981a [35], 1981b [36]; IETF, 2007 [27]). This is illustrated by Figure 2. However, Location Information is not the contents of a voice or SMS communication (IETF, 2007 [27], 15 [3.]). Legally, LI is considered to be information about a customer, and as âtelecommunications dataâ. This is evident from the legal phrase: âthe affairs or personal particulars (including any unlisted telephone number or any address) of another personâ (TIA Act, 1979 [14], s 276). Location Information is not legally regarded as the content of a communication in Australia, unfairly denying this aspect of LI, whereas LI may be both content in itself and information related to voice content. Instead, location information is regarded as subscriber related data, as metadata, as telecommunications data, as information related to the contents of a communication (Parliamentary Debates, 2016 [37]; TA 1997 [38] ss 275A, 276, 280, 313(3)(4)(7); TIA Act 1979 [14] ss 187A (1), 187AA (1) items 1â 6, Chapter 4 Part 1 Division 3-4; LCARC, 2015 [39], 27).

From a technological perspective, the traditional metadata versus content distinction is difficult to apply to the IP-mediated LTE network when it comes to the retention and disclosure of LI, in American law (Bellovin *et al.*, 2016 [24], pp. 2, 3, 8, 17) and in terms of Australian electronic surveillance law and policy, as contained in *TIA Act 1979* [14] and the *TA 1997* [15].

The *CAC Determination 2015* [25] sets out the metadata collection procedure to be used. This allows the Agencies to access the information about the voice call or SMS. The Agencies issue authorisations and notifications requesting access to the LI (*CAC Determination 2015* [25]). Leonard (2015c [40], p. 7) referred to this process as self-certification. The *TIA Act 1979* [14] addresses how the content of the call is to be accessed, given the sensitivity and personal nature of the call (Leonard, 2015c [40], p. 7). A domestic preservation notice and a stored communications warrant or an interception warrant are required to access the contents of the call (Leonard, 2015c [22], pp. 8-9; TIA Act, 1979 [14] ss 39, 109, 110, 110A, 115). Leonard (2015c [40], p. 10) stated, given the popularity of smart phones with built in geo-located cellular abilities, information about communications over those phones reveal details of peopleâs lives, and the value of this cannot be underestimated. This trend has led Australia to adopt the data retention scheme requiring the Telco to retain the data about a phone call or SMS (Leonard, 2015c [40], p. 10). This smart phone use trend is enabled by the geo-located cellular abilities of telecommunications networks, such as the IP-mediated LTE network. Unlike the copper wire system, an IP-mediated LTE network uses the Internet to carry both the contents of the voice call and the information about the communications (IETF, 2007 [27], p. 6 [1.2]). The telecommunications data retention scheme requires LI be retained and disclosed to the Agencies, in the same way it was done for copper wires (Leonard, 2015c [40], pp. 7, 10). The Australian telecommunications law, which allows for access to LI, with the newly introduced privacy safeguards as per the *CAC Determination 2015* [25], must therefore be assessed for vagueness and broadness, as to whether it sufficiently protects privacy. This is needed given the popular use of smart phones, which track the location of the device and reveal personal habits and traits, coupled with the discretion granted to the Agencies and the Telco, even though LI may not be voice content. The more fundamental question is: if LI is carried inside an IP packet, as a message, would this not make the LI the content of a communication in itself, even though it may be related to the voice call because the LI is generated at the time the voice call is made? If so, should LI be protected as the content of a communication exchanged within the network, as illustrated in Figures 1 and 2, given it reveals SI and PI about the individual, equally sensitive as the contents of a voice call message? This would require an analysis of the legal definitions of terms such as âcommunication(s)â and âinformation related to the contents of a communicationâ (TIA Act, 1979 [14] s 276). This analysis must be done in relation to how LI is legally classified as subscriber data, but is, as a matter of fact, technologically carried as the content of an IP packet and simultaneously reveals SI and PI. The potential dual nature of LI, both as a content and as information related to the voice call needs to be legally and technologically deciphered. Disregarding the content nature of LI and legally classifying LI simply as metadata, not only has the effect of denying the true nature of LI, but is not rooted in how the modern Internet-based communication network operates. This policy position may be entrenching the existing powers of the Agencies, despite being based on how an outdated analogue fixed-line copper-based network was designed and operated.

Packet Neutrality

As discussed above, the *TIA Act 1979* and the *TA 1997* are not technology neutral in that they do not treat all types of PI with the same privacy protection standards. The Attorney-Generalâs Department (AGD), however, stated that the *TIA* must remain technology neutral (Department of Parliamentary Services, 2007 [41], 7-8 14). Section 187AA (1) items 1â6 of the *TIA Act 1979* and section 275A of the *TA 1997* treat signal messages carrying LI inside SCTP/IP packets (*see Figure 2 below*) differently from the Transmission Control Protocol (TCP)/IP packets carrying voice or SMS communications. Voice content is also able to be carried in SCTP/IP packets (IETF 2007 [27]).

[42]

Figure 2. The structure of the SCTP, demonstrating the connection between two connected devices to carry SCTP messages (IETF, 2007 [27], 6 [1.2]).

The IP packets carrying voice or SMS communications must only be stored with a domestic preservation notice and be disclosed and accessed only with a stored communications warrant (TIA Act, 1979 [14] ss 39, 109, 110, 110A, 115). The SCTP/IP packets carrying LI are instead subject to mandatory data retention, without the need for similar protection to be disclosed and accessed only with a stored communications warrant (TIA Act, 1979 [14] ss 39, 109, 110, 110A, 115). Instead, it may be accessed with a self-certification authorisation and notification under the *CAC Determination 2015*.

The *TIA Act 1979* and the *TA 1997* should be packet neutral to both types of IP packets, so as not discriminate against LI by granting it less privacy protections under the *CAC Determination 2015* because LI is not the contents of a voice or SMS communication and is not carried in TCP/IP packets. The contents of TCP/IP packets and SCTP/IP packets both reveal PI and SI about the individual, and this may need to be the standard under which privacy must be better protected. The research questions raised in the section above are equally relevant to this discussion.

Greater Location Precision

The Agencies are granted access to coarse LI (Evidence to PJCIS, 2015 [43]), but the coarse LI from a modern IP-mediated LTE network generates and reveals more precise locations than earlier networks (Nohrborg, 2017 [44]). The coarse LI are the radio measurements or positioning measurements. The radio measurements or positioning measurements are the location estimates of the mobile device as generated by the IP-mediated LTE network itself, without the Telco analysing the location estimate to, for example, narrow down the location estimate from 100 m from the cell tower, to 50 m. The Telco is not required to analyse the location estimate to narrow the location of the mobile device from 100 m to 50 m. The Telco is simply required to disclose the 100 m location estimate to the Agencies. However, given that E-UTRAN is a new Radio Access technology, and is not reliant on older technologies, this enables the UE to be located with greater accuracy. E-UTRAN is planned to be technology neutral and robust for the future as 5G LTE networks are rolled out, in providing more precise geographic locations by using the Global Navigation Satellite System (GNSS): âthe E-UTRAN positioning capabilities are intended to be forward compatible to other access types and other position methods, in an effort to reduce the amount of additional positioning support needed in the futureâ (ETSI, 2017g [45], 12 [4.1]).

To better protect privacy, it needs to be recognised that the LI carried in a modern IP-mediated LTE network reveals more precise locations of the mobile device and of the individual user. This is also made possible by the use of femtocells that reveal more precise LI than traditional analogue and fixed-line telecommunications (Germano, 2010 [46]; ETSI, 2017a [23], 43 [8.1.3.2.1]; ETSI, 2017b [47], 20 [3.1]; ETSI, 2017c [48]).

Privacy is Not Adequately Protected

Selvadurai, Gillies and Islam (2009 [49]) stated the operation of the *TIA 1979* [14] threatened fundamental privacy interests. Privacy is not adequately protected (Michael & Clarke, 2012 [50]). In the view of Michael and Clarke (2012 [50]), privacy laws are eroded by exceptions and location privacy is not specifically addressed in any Australian law. Fernandes and Sivaraman (2015 [51]) also argued the Australian data retention law passed in 2015 strengthened protections for privacy. This claim was made without adequate analysis of the powers of the Agencies, the role of the Telco and the oversight limitations and exceptions placed on the Agencies in relation to LI. Reference was made to Internet of Things (IoT) devices, claiming that the retention laws may negatively impact privacy due to the deployment of IoT devices, but no specific mention was made of the significance of the LI of IoT devices. Zwolenski and Weatherill (2014 [52]) warned of the security and data protection pitfalls of IoT devices, but not in relation to the duties of the Telco to retain and disclose GPS data, and how mobile devices use the IP-mediated LTE network to create and exchange LI. Carona, Bosua Maynard and Ahmad (2016 [53]) examined the individual privacy risks posed by IoT, in relation to the Australian Privacy Principles (APP). Two risks identified related to the collection of data by means of unauthorised surveillance and uncontrolled data generation and use. Unauthorised surveillance was defined as the collection of mass data, which inferred the extensive tracking of individuals. The tracking is done without prior or informed consent. This definition did not make it clear whether access and use by the Agencies was considered unauthorised surveillance, seeing that the prior consent of the individual is not required for the Telco to retain and disclose LI (Carona *et al.*, 2016 [53]). Carona *et al.* (2016 [53]), however, admit that law enforcement bodies and the government comprise those parties that are involved with IoT data protection. The conclusion reached was that individual privacy is insufficiently guarded (Carona *et al.*, 2016 [53]). The data considered included LI, call history, movement and software applications collected from smartphones as the type of sensor, and its use for criminal investigations and fraud (Carona *et al.*, 2016 [53]). Carona *et al.* (2016 [53]) did not consider the APPs from the perspective of Australiaâs mandatory metadata retention and disclosure perspective, nor did they conduct a legal analysis.

Statutory âprivacyâ jurisdiction is reliant on the existence of PI as per the*Privacy Act 1988* (Cth). Australian common law is said not to recognise the general right to privacy (Taylor, 2000 [54]: 238, 241; Human & Constitutional Rights Resource Page, 2018 [55]; the *Victoria Park case*, 1937 [56]; the *Lenah Game case*, 2001 [57]). Privacy is protected as a by-product of other interests that are already protected, such as confidentiality clauses from contracts with banks (Taylor, 2000 [54]: 240-241).[iii] [58] Customers of Telcos are protected by privacy policies and standard terms and conditions that contain clauses to protect the privacy of the customers, and also under the *Privacy Act 1988* (Cth) (Vodafone Hutchinson Australia, 2017 [59]). Lachmayer and Witzleb (2014 [60]; 768) wrote that the powers of the Agencies were extended in âhyper-legislationâ because of the 9/11 attacks, with significant negative impacts on privacy, due to Australiaâs lack of a constitutional right to privacy (Roach, 2011 [61]). Bloch and Wark (2015 [26]) suggested that the increased data collection and access powers are unjustified as they intrude into the private lives of individuals. The authors Davies (2001 [62]), Williams (2005 [63]), Golder and Williams (2006 [64]), Bramwell (2012 [65]), Nicholson and Redlich (2015 [66]), Leonard (2015a [67], 2015b [68]), Fair (2015 [69]) and Leonard (2015c [40]) generally focussed on writing about the negative impact on privacy as a human right, because of the power to access retained telecommunications data without a judicial warrant. Rodrick (2009 [70]) wrote about the negative impact on privacy of mobile phone data location access and use. Rodrick (2009 [70]) discussed GPS and cell identification as methods of cellular device location approximation. The studies of these authors predate the introduction of the data retention scheme in 2015. In 2009, less detail was publicly revealed about the types of information to be retained. Privacy must now be studied in the context of PI in terms of the revised *Privacy Act* [10]. After 2015, Shanapinda (2017 [71]) argued the collection of LI from social network websites also aims to complement the LI collected by the Agencies and undermines privacy safeguards such as those contained in section 180F of the TIA Act, 1979 [14].

The Privacy Test

In terms of section 180F of the TIA Act 1979, the AFP, but not ASIO, must be satisfied on reasonable grounds that any interference with the privacy of any person that may result from the disclosure or use of the âinformation or documentâ is justifiable and proportionate. This is the privacy test to be applied. Section 180F of the TIA Act 1979 refers to the proportionality principle, which lays the basis of using privacy itself as a tool to limit the powers of the Agencies. In other words, only LI, that is PI that is proportionate and justifiable, must be collected and used â nothing more. Selvadurai (2017 [72]) concluded that the post-2015 Australian framework that allows for access to telecommunications data was drafted in a manner that sought to overcome the privacy challenges the European Union (EU) faced. Selvadurai (2017 [72], pp. 35-41, 36) referred to the EU Data Retention Directive (Directive 2006/24/EC [73]) that was invalidated by the European Court of Justice (ECJ), stating that, given this legal precedent, it is interesting that Australia requires the retention of specific kinds of telecommunications data. Selvadurai (2017 [72]) questioned whether the retention of telecommunications metadata was a necessary national security initiative or a disproportionate interference with personal privacy, by analysing the Australian framework in relation to the ECJâs decision, given the similarities. Selvadurai (2017 [72], pp. 35-41, 36) 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 [72], pp. 35-41, 37) described the scope of the statute to analyse the effectiveness in calibrating the privacy and national security interests. This review proposes an assessment about whether the Australian framework can really be said to have overcome the privacy challenges, based on the functionality of the IP-mediated LTE network, as discussed in previous sections, critically analysing in detail the privacy safeguards introduced in 2015, based on BLD analytics. In other words, given the use of automatic data processing of the LI, as discussed in the section titled âThe Use of Big Data Analytics Software and Governanceâ, is the retention and collection of LI for two years justifiable and proportionate?

The questions that future research may study include:

- given the broad inquiry and investigatory powers;
- the less stringent access rules; and
- given the broad meaning of national security as discussed in existing court cases, such as the *Jaffarie* [19], the *Farrel* [18], the *Day* [20] and the *Samsonidis* [21] court cases;
- the use of BLD analytics; and
- coupled with the lack of transparency,

what volume of LI retained and disclosed is proportionate and justifiable to ensure public safety, based on the risks posed?

Given the circumstances above, is privacy adequately protected? Is privacy a strong enough tool to effectively limit the powers of the Agencies or is privacy placed in a conflicting position, making it almost impossible to effectively restrict the powers of the Agencies?

The Privacy Protection Principles versus the Broad Investigatory Powers versus Public Safety

Clarke (2015 [74], 2016 [75]) proposed the âMeta-Principles for Privacy Protectionâ framework.Clarke (2016 [75]) proposed a privacy impact analysis in respect of data retention implementation. The principles include: evaluation, consultation, transparency, justification, proportionality, mitigation, controls and audit (Clarke, 2016 [75]). Clarke (2015 [74]) described the 2014 data retention proposal before the law was passed in 2015. After the *Data Retention Act 2015* [11] was passed, the principles of transparency, justification and proportionality were incorporated into the privacy safeguards, and now require an empirical analysis.

Selvadurai, Kisswani, and Khalaileh (2016 [76], p. 229) simply described the Australian interÃception law reform process in relation to the proportionality principle. The reforms were justified on the basis of enhancing legislative longevity, due to the persistent changes of telecommunications technologies (Selvadurai *et al*., 2016 [76], p. 230). However, as illustrated by the digital and mobile transformation of communications, from analogue and fixed-line communications, laws may lose touch with reality and continue to grant more powers to the Agencies due to the advancements in communications technology. Keeping the laws unchanged does not allow for a check-in to assess the impact of these technological advances, as discussed in previous sections. Selvadurai, Kisswani, and Khalaileh (2016 [76]) assessed the application of the proportionality principle. This was done specifically with regard to conducting interceptions, and not access to LI in relation to technological convergence and âheightened national securityâ (Selvadurai *et al*., 2016 [76], pp. 230, 239). In the context of telecommunications law, the proportionality principle was described as weighing up potential threats to âpublic security against possibly breaking the rights of the person â the aim is to ensure that collecting the content is reasonably proportionate to the desired goalâ¦.â (Australian AGD, 2012 [77], p. 26). The concept of âpublic safetyâ refers to the safety of the public (Australian AGD, 2012 [77], p. 26; Selvadurai *et al*., 2016 [76], p. 232). Selvadurai *et al.* (2016 [76], pp. 231-232) noted that the concept of security is broad and open to interpretation, but did not analyse the *Jaffarie* [19], the *Farrel* [18], the *Day* [20] and the *Samsonidis* [21] court cases.

Selvadurai *et al.* (2016 [76], p. 229) placed emphasis on the âlikely threatâ. However, the powers of the Agencies involve investigating persons, to determine if they may pose a security threat: â(a) â¦ undertake inquiries to determine whether a particular subject or activity is relevant to securityâ (Attorney-General's Guidelines [78], s 6.1.). In regard to description bySelvadurai *et al.* (2016 [76], p. 229) of the âproportionality principleâ, it appears that the powers of the Agencies are defined, insofar as the Agencies seek to investigate or conduct an inquiry in circumstances where there is no âlikely threatâ. However, the LI is collected to assess if a person may pose a threat in the future, and the collection of the LI is not always legally required to be based on reasonable suspicion or on goodwill, to determine if a person is relevant to security. There is a requirement for the AFP to have an âinvestigationâ in order to collect prospective location information (TIA Act, 1979 [14] s 180(4)). If the AFP is requesting access to prospective location information for a serious offence or an offence against the law of the Commonwealth that is punishable by imprisonment for at least 3 years, the AFP needs to have suspicion of a past, present or future serious offence, based on reasonable grounds, to collect prospective location information (CAC Determination 2015 [25] Part 3 s 3.01 (1) Item 3(c) (viii), (ix)). It is, however, only when it comes to serious offences that the AFP is required to conduct an âinvestigationâ and have suspicion of a past, present or future serious offence, based on reasonable grounds (TIA Act, 1979 [14] s 180(4)*; CAC Determination 2015* [25] Part 3 section 3.01 (1) Item 3(c) (viii) and (ix)). It follows that, for minor offences, historical location information may be collected without a suspicion of a past, present or future serious offence, based on reasonable grounds.

It is only in respect of prospective location information for serious offences that the short description of offences is required to be stated in the authorisation under the *CAC Determination 2015*, and only in respect of the AFP. It is only in respect of prospective location information for serious offences that an âinvestigationâ of offences is required, and only in respect of the AFP (*CAC Determination 2015* [25], Schedule 1 Part 2 s 2.02 (1) Item 8). It also follows that, for serious offences, historical location information may be collected without the suspicion of a past, present or future offence, based on âreasonable groundsâ. In other words, no reasonable grounds are required to collect the historical location information under the *CAC Determination 2015* for serious offences (TIA Act, 1979 [14] s 178(2); *CAC Determination 2015* [25] Part 3 section 3.01 (1) Items 1- 6). The AFP does not need to have an investigation as a requirement before collecting the historical location information for a serious offence (TIA Act, 1979 [14] ss 6A, 6B). There seems to be no requirement for the AFP to have an active âinvestigationâ, as defined in the *Day court case* [20], as a requirement to collect historical location information. It means the AFP does not need to have a suspicion of a past, present or future offence, based on reasonable grounds, to collect the location information when it is putting the facts together about the actions of the individual in order to allege that the person has committed a crime. Given these broad investigatory powers, the Agencies may collect and use LI under the less stringent requirements of the *CAC Determination 2015*. The two conflicting interests can be still better balanced than they are at present by requiring reasonable suspicion and a judicial warrant. Without the latter more stringent requirements but pending a rigorous study, it may be said that privacy appears to be unfairly compromised in favour of âpublic safetyâ.

It may be said that it appears that the privacy safeguards introduced after 2015 continue to be threatened by the fact that the Agencies continue to self-certify the authorisations, as they have always done when copper-wire landline telecommunications was in use (Evidence to PJCIS, 2015 [43], 31). This is despite the revealing nature of the modern IP-mediated LI. A detailed study, based on the legal powers, contrasted against the oversight mechanisms and the functionality of LI may potentially support the above argument. The proportionality test can then be critically analysed in this relevant context of self-certification and âpublic safetyâ.

Lack of Transparency

Williams and Hardy (2014 [79]) stated metadata access is not transparent - disclosing that ASIO collecting data for special intelligence operations is a criminal offence. This poses risks to media freedom. Rix (2013 [80]) studied ASIO investigations about the questioning and detention of suspects and the power to keep the information about this secret. Rix (2013 [80], p. 240) objected to the claims for secrecy, arguing âthere can be little dispute with the assertion that some level of secrecy is required by ASIO to enable it to deal effectively with the terrorist threat. It is far more difficult to accept that complete secrecy, and no accountability, equates to watertight securityâ. Rix (2013 [80]) went on to state that the public is not able to scrutinise the powers of the Agencies due to the level of secrecy. Sarre (2017 [81], p. 176) states it is still too early to determine whether the telecommunications data retention laws are effective, given the confidential nature of the investigations. In respect of ASIOâs confidential access to LI, the lack of transparency makes it difficult to assess whether the Agencies are complying effectively with the privacy safeguards at the time of collecting the LI, and whether the actions of the Agencies are reviewed in a sufficiently open administrative and judicial systems afterwards. The lack of transparency contributes to the self-serving character of the LI retention and disclosure framework. The Telco is prohibited from informing the person of the LI collected about them (TIA Act, 1979 [14] ss 181A (1), (2), (4), (5); 181(B1), (2), (4), (5); 182A (1), (2)). The collection of the LI is a confidential process (*CAC Determination 2015* [25] Schedule 1, Part 3;TIA Act, 1979 s 108(1) [14]). The individual is not informed of the LI requests and disclosures. In replying to the PJCISâ comment that the Journalist is not informed about the application for a Journalist Information Warrant (JIW), the Attorney-General replied that a person under investigation may destroy evidence if informed and frustrate the investigation (Letter from the Attorney General [82], 9 February 2016). However, the lack of transparency has a profound impact on the ability of the individual to try and assert their privacy. There is little or no opportunity for an individual to become aware that the LI may have been misused. There is little or no opportunity for an individual to know that only LI that was reasonably necessary and proportionate was collected. For the person to lodge a complaint they would need to be aware of the privacy breach of section 180F. The affected individual would find it challenging to collect copies of the authorisations and notifications to challenge the Agencies and whether and how they met the post-2015 privacy tests. It is significant that the oversight bodies such as the Office of the Inspector-General of Intelligence and Security (OIGIS) and the Commonwealth Ombudsman conduct their investigations based on complaints (IGIS Act 1986 [83] (Cth) ss 10, 11, 12*; Data Retention Act* [11] Schedule 3). However, obtaining the information necessary to identify a possible privacy breach and to make a credible and specific complaint is practically almost impossible. Can privacy be said to be adequately protected under these circumstances? The workings of the oversight bodies may require further scrutiny.

Less Stringent Oversight Measures and the Broad Powers

Leonard (2015c [40]) did not address how the broad investigatory and discretionary powers of the Agencies to collect LI, and the discretion of the Telco to voluntarily retain and voluntarily disclose LI (TIA Act, 1979 [14] ss 177(1), 178(3)), interacts to create an environment that subjects the privacy of the individual to the commercial and law enforcement interests, and without providing sufficient privacy safeguards. Enhanced accountability was introduced in the form of greater legislative oversight, with the granting of additional supervisory powers to the Commonwealth Ombudsman (TIA Act, 1979 [14] Schedule 3). This included the complaint procedures. As stated in the section above, the lack of transparency makes lodging complaints difficult, potentially weakening the oversight and protecting privacy poorly.

The powers of the Agencies are also broad because LI is not classified as âcontents of a communicationâ. LI is classified as âmetadataâ, and less stringent requirements are applied to access and use LI (TIA Act, 1979 [14] s 275A; LCARC, 2015 [39], p. 77 [71.182]). The *CAC Determination 2015* [25] is the less stringent procedure that is used to access LI. Burgess (2015 [84], pp. 16-17) argues new âmetadataâ laws are vital for the police. There is no doubt about the value of the LI. The Agencies can still perform their functions effectively using valuable LI, but privacy can still be better protected than it is currently protected under the *CAC Determination 2015* [25], by amending the self-certification process and introducing a judicial warrant to access and use LI.

In 2012, Svantesson (2012 [85], pp. 268, 275) described how private data could be accessed in Australia for specified purposes, as opposed to bulk data collection. Accessing data for a specific purpose appears to be a myth. The LI can be collected for broad purposes if they are related to undefined police activities and functions. As stated in the paragraph titled âThe Privacy Protection Principles versus the Broad Investigatory Powers versus Public Safetyâ, this may pose unfair risks to privacy. Svantesson (2012 [85], pp. 270â271) referred to the Attorney-Generalâs Guidelines to be followed regarding access to the data, distinguishing between requests for data and voluntary disclosure, and stated the Agencies were generally compliant with the laws when accessing and using telecommunications data. However, an oversight tool, such as the *CAC Determination 2015* [25] that is used to protect privacy, may be more permissive than it is restrictive, and have such a low threshold that the Agencies are able to easily comply. Sarre (2017 [81]) argues that the Agencies are generally compliant with the laws, and states the Agencies use their powers for the purposes of security and law enforcement. The powers are broad and therefore compliance is easier due to the low access threshold. The oversight test used only inspects the âextentâ of compliance, which may send the message that non-compliance is accepted and condoned (*Data Retention Act* [11] (Cth), s 186B).

Jones (2016 [86]) argued Australian intelligence is imprecise because it is subject to political distortion. The expanding legal powers, in Jonesâ view, have evolved into a national security state that exacerbates domestic accountability issues. Jones (2016 [86]) did not explicitly analyse the powers of the Agencies in relation to the IP-mediated LTE network, in terms of how the network locates the mobile phone with greater precision and reveals PI and SI. Jones (2016 [86]) did not contrast the revealing nature of the network against the Attorney-Generalâs Guidelines [78] and the *CAC Determination 2015* [25]. These two documents do not contain clear restrictions about inquiries and investigations that have political and racial angles, to ensure good faith. The two documents also do not clearly address how the Agencies can prevent bias and prejudice to avoid potential misuse. In the *Jaffarie case* [19] (16 [17]), the court relied on section 20 of the *ASIO Act* 1979 [87] as preventing undue influence from the outside but did not question whether any internal processes exist and are applied to address biases of officers themselves and undue influence from the outside.

Telecommunications Data as Personal Information

Telephone metadata is valuable in making inferences that are of a sensitive nature(Mayer, Mutchler and Mitchell, 2016) [88]. Mayer *et al.* (2016 [88]) assessed the privacy characteristics of telephone metadata, using a crowdsourcing methodology. The study concluded that telephone metadata was âdensely interconnectedâ and re-identifiable â this even though the privacy protections of telephone metadata are not significant, and the bulk telephone metadata collection program of the National Security Agency (NSA) relied on data that is not considered âPersonally Identifiable Informationâ (PII) (Mayer *et al*., 2016 [88]). Using the location histories of the participants, re-identification of the participants was performed using location data from social networking sites.[iv] [89] The researchers could often make inferences regarding the geo-location of the participantsâ residences from call and SMS data. The location data did not disclose exact locations (Mayer *et al*., 2016 [88]). Locations could, however, be inferred by re-identifying the business the participants called, supported by location addresses from the websites, and using this information to guess their residential premises. The final step was to use the Google Geocoding API[v] [90] to assess the longitude and latitude of the businesses and homes (Mayer *et al*., 2016 [88]). If privacy is to be appropriately protected, the law must recognise that LI is generated and exchanged as a communication that reveals more precise location estimates, and PI and SI about the individual. If the voice or SMS communication is made via a femtocell, the location estimate of the eNB selected to handle the communication can be just as precise as if signal strengths from various towers were used. The Telco is practically made to retain LI that was selected by the femtocells deployed inside and outside homes to boost the cell phone coverage (Germano, 2010 [46]). If the femtocellâs signal is the strongest, the cell phone will connect to the femtocell (Battersby, 2012 [91]). The precision of these base stations can be within a range of 100 meters, such as the Vodafone site at the University of New South Wales (UNSW) (ACMA 2017 [92]a). Electronic Frontiers Australia (EFA) argued mobile phone location accuracy approximates 200 to 100 meters in metropolitan and urban areas. Electronic Frontiers Australia (EFA) argued Assisted-GPS would greatly improve mobile phone LI (Department of Parliamentary Services, 2007 [41], 14). The LI is disclosed raw and unprocessed, but that means a 100 m coverage radius for finding a person. It is no longer like looking for a needle in a haystack, but more like using a microscope. Given the development of modern IP-mediated communications technologies, with base stations that are nearer to each other and the coverage radius smaller in urban areas, the licensing and use of femtocells with a proximity radius of 100 m, and the popularity of smart phones with satellite positioning ability, the reliance on this traditional content versus metadata distinction may be working to the benefit of the Agencies and compromise privacy protections. The scales are thereby subtly skewed in favour of the powers of the Agencies rather than adequately balancing the more revealing nature of modern-day mobile communications. To gain access to use LI is more flexible than under the traditional rules prescribed for warrants and domestic preservation notices. As a result, LI may need to be protected in the same way as the contents of a communication, under the legal system, given that all these types of communications reveal PI and SI.

The Dual Nature of Telecommunications Data

Johnston (2017 [93], pp. 82-83) advanced the argument that LI cannot be about just one thing but can also be about the individual and therefore be PI. In the *Telstra Corporation Limited case* [16], the Deputy President decided telecommunications data not used for billing purposes, and from which the identity of the person is not obvious, is not âaboutâ the individual and is therefore not PI. Johnston (2017 [93]) argued that this was a narrow and binary formulation. The information need not be about only one phenomenon or aspect. Johnston (2017 [93]) argued that this decision might result in entities denying their privacy obligations by arguing that the information is strictly âaboutâ the service, such as banking transactions or medical procedures, to the exclusion of the privacy rights of the individual. This review agrees with Johnston (2017 [93]). The Administrative Appeals Tribunal (AAT) dissected how the technology operates, but then took a very technology-driven and narrow interpretation. LI is inherently designed to track the mobile device in the IP-mediated LTE network in order to deliver the communication to the device, as illustrated by Figure 1. However, LI can be applied for a myriad of other purposes, especially when aggregated using BLD analytics technologies, to reveal PI and SI. The later decision of the Federal Court: the *Privacy Commissioner case* [17], that stated information can be about a myriad of things, requires greater scrutiny in the BLD and IP-mediated LTE network contexts, in relation to the Attorney-Generalâs Guidelines [78] and the *CAC Determination 2015* [25], as governance tools. According to the *Telstra Corporation Limited case* [16], any other application of the telecommunications data generated does not alter the primary purpose and functioning of the technology, even if the telecommunications data is matched with other external information and reveals habits about the person, the residence of the person or details about the work-related activities of the person. The information cannot be just about one thing. The *Privacy Commissioner case* [17] planted the seed for the idea that the LI may not just be about the primary purpose of delivering communications. If the facts can demonstrate that the LI was matched, and the identity of the person was revealed or is reasonably ascertainable, by the LI that tracked the mobile device, whether it delivered the voice call or whether there was no voice communication to deliver, the LI can also at the same time be about the individual (Privacy Commissioner case [17] 16 [63]). Unlike the AAT, the Federal Court accepted that the information can be about various things: âInformation and opinions can have multiple subject mattersâ (Privacy Commissioner case [17] 16 [63]).

A single piece of information that starts out by not being about a person may end up being about a person when it is combined with other separate pieces of information (Privacy Commissioner case [17] 16 [63]). If the pool of LI is combined with extra information, the LI may end up being PI. The Federal Court stated, based on the facts of every case, at first, it must be determined whether every single item of information or the combined pieces of information requested from the Telco are about the individual (Privacy Commissioner case [17] 16 [63]). Secondly, once having determined that the information is about an individual, in order to determine whether the identity of the person is reasonably ascertainable, one must then make an evaluative conclusion. The Federal Court stated that aggregated information may be about an individual, even if a single piece may not be about an individual (Privacy Commissioner case [17] 16 [63]). The Federal Court differentiated between a case of an identity that is obvious from the information, and a case where the identity may not be apparent. As illustrated by Figures 1 and 2, LI is inherently designed to be about tracking the mobile device in the IP-mediated LTE network, with the view of delivering the communication (the location information contained in a message) to the mobile device or the Location Server or the SEDNode web portal from where the LI is downloaded and given to the Agencies (iiNet, 2015 [94]). However, LI may be applied to a myriad of other purposes and, as such, the LI forms various relationships that end up being about the individual. The primary design and purpose of LI remains, but that does not exclude other relationships. The LI may start out being about the delivery of the voice and SMS communication to the recipient, as it is exchanged via the Network Elements, such as the Location Server, as illustrated in Figure 1, but a new relationship is formed with the individual at the secondary level, when the LI reveals the physical location of the mobile device and in turn that of the individual, leading to opinions being formed about the character of the person. The LI now serves a secondary purpose, but still an important purpose that may require greater privacy protection, under more stringent requirements than what the *CAC Determination 2015* provides.

The Use of Big Data Analytics Software and Governance

To Moses and Chan (2014 [95], p. 645) Australia was starting to recognise the potential of Big Data (BD) analytics for the enhancement of national security. In BLD analytics, various pieces of information are aggregated to reveal new information that can be used in investigations by the Agencies. Chan and Moses (2017 [96]) explored the likely impact of BD technology in relation to the Australian law enforcement and national security landscape. Chan and Moses (2017 [96], p. 300), and Smith, Moses and Chan (2017 [97]) made the clarion call for a better understanding of BD analytics technology, its challenges, its uses and influence, and its proper governance and regulation. BD analytics is about establishing connections by using new software and hardware technologies to analyse huge sets of diverse data (Maurushat, 2016 [98], p. 2). Maurushat (2016 [98]) described the perceived advantages, risk and challenges around BD and its uses by the Agencies. The uses related to being able to âpredictâ and investigate criminal and intelligence incidents (Maurushat, 2016 [98], p. 1). The risks associated with such use included the threat to privacy and the erosion of trust (Maurushat, 2016 [98], pp. 9-10). Selvadurai (2017 [72]) described BD as valuable to the Agencies, referring to the benefits of identification of associations between communicators, providing a precise digital profile, and matching the data with data obtained from social media to identify persons who are relevant to security or suspected of having committed an offence. Selvadurai (2017 [72]) argued this undermined privacy protections. Shanapinda (2017 [71]) argued the public has a legitimate expectation not to be tracked online by the Agencies, when describing the application of BD analytics over retained data, and then merged with open source intelligence (OSINT), for investigations. Privacy is impacted at the time the LI is retained â the PI about the individual is stored. Privacy is again impacted at the time the LI is disclosed to the Agencies â the PI about the individual is shared. Privacy is impacted again at the time the LI is analysed using BLD analytics, to reveal PI about individuals. The BD analysis is automated processing of the LI, and with greater efficiency than previous manual operations. There is no telling what treasures two yearsâ worth of LI may reveal about the individual. There is no telling how relevant the PI that has been revealed is to the investigation or inquiry in question. The *CAC Determination 2015* does not regulate how the data collected and PI revealed may be treated and applied to the investigation at hand. The extra PI revealed is open to the risk of misuse, to aid the investigation. The newly revealed PI may broaden the scope of the investigation that can potentially incentivise Agencies to continue indefinitely to use the PI to find something criminal against all odds, whether minor or serious, instead of dropping the inquiry or investigation. Under a judicial warrant, the scope of the inquiry or investigation would be clearly defined and authorised. Under the *CAC Determination 2015*, however, the Agencies can bypass such a narrowed scope â leading to scope creep. Throughout all this, the PI is retained indefinitely by the Agencies, and this too impacts the privacy of the individual. The ease with which LI is available to the Agencies for two years, that the LI can be collected from the Telco, and that the LI can be processed by automated means to disclose PI and SI are the sorts of circumstances that may impact privacy heavily. The safeguards adopted in 2015 may therefore be inadequate to protect privacy. It may be justifiable and proportionate that a two-year history of the person be revealed, in order to keep the public safe, but could a weekâs or a monthâs history do? The *CAC Determination 2015* is silent on these sorts of governance issues, and does not offer such guidance.

Unfair Limits to Civil and Property Rights

To better protect privacy, the Telco is not required to retain LI when the individual is not making a call. As an exception, the Telco may only retain LI at the start and at the end of a communication. This is commendable, but the Telco may, however, legally retain this LI voluntarily (TIA Act 1979 [14] ss 187A (1), 187AA (1) item 6). To the AGD, this reduces the level of detail because the Telco is not required to retain the regular continuous records of the location information:

[T]he nature and volume of location information that service providers will be required to keep has been strictly limited to ensure that service providers are not required to keep continuous records about the location of a device, or anything approaching that level of detail (PJCIS 2015 [99], 93 [3.79]).

The detail of LI to be retained is therefore dependent on whether the person uses the mobile device to make calls or to send an SMS. This position sends the message that, if a person wants less LI about their communications to be retained and want less PI about them retained and disclosed, then the person should reduce their level of communication with their friends, families and other associates. Mobile devices are popular and people are dependent on these devices (ACMA, 2017 [92], 17). Not using the device or reducing its use would be a form of self-censorship and create a chilling effect on civil and political rights. This impacts the affected personâs privacy and free speech, to communicate at will, when and how they like, and not to be concerned that, if they speak too often, the Telco would retain more LI than they would be comfortable to disclose to the Agencies.

The individual must also be wary about the location from which to communicate. The person seeking to protect their privacy may limit their movements or choose not to carry their mobile device with them for fear of being tracked. The freedom of movement of the person is indirectly curtailed. The person would also be unfairly restricted from enjoying and exercising full ownership over his or her private property. The psychological impact is another factor to consider: the fear that is created and the mental health effects of being under constant surveillance with every communication made and every location entered. These are the negative impacts of the LI retention and disclosure framework that may be studied further.

Analysis and Recommendations for Future Research

The traditional argument from the authors cited has been to criticise the powers of the Agencies to access and use information collected from the Telco, in relation to privacy. As stated above, this information includes LI, which reveals PI and SI about the individual user. It is therefore known that the powers of the Agencies impact the privacy of the individual. However, privacy is rarely studied from the perspective of being a tool used to help limit the powers of the Agencies. Many authors have written about the impact on privacy of the powers of the Agencies, but not about the powers and the limits on those powers in the period from 2015 to date, and not in enough detail about how modern technologies operate. This was a period where the powers of the Agencies came under the public spotlight as the Agencies renewed their commitment to better protect privacy, while simultaneously seeking new powers to collect retained LI (TIA Act 1979 [14] s 180F; *CAC Determination 2015* [25]). The duties imposed on the Telco to retain LI for two years, coupled with the discretion to also retain more LI for commercial purposes, are an essential component of the changes made since 2015 and they require empirical investigation, in order to confirm what reasonably appears to be, from the discussions above, a negative impact on privacy.

As legal and policy positions change, the context and status of these frameworks evolve. For a better contemporary understanding, the recent changes require investigation to assess their modern impact on privacy in the new environment, as opposed to continuing to rely on outdated concepts that may be decreasingly relevant to emerging practices. At the same time, privacy is also a check on the powers of the Agencies (TIA Act 1979 [14] s 180F; *CAC Determination 2015* [25]). The Agencies are entrusted with safeguarding privacy interests as well as pursuing law enforcement interests to obtain, access and use LI (TIA Act 1979 [14] s 180F; *CAC Determination 2015* [25]). The *TIA Act 1979* [14] classifies LI as subscriber data and as metadata,[vi] [100] despite the revealing and sensitive characteristics of LI (APC, 2015 [101], 42 Appendix B [8]). This means the Agencies can access LI under less stringent requirements than the contents of a voice or SMS communication (*CAC Determination 2015* [25]; TIA Act 1979 [14] ss 107H, 108(1)). The proposed research can investigate how the powers of the Agencies and the revised privacy safeguards are aligned. The research can confirm the fact that privacy is the most vulnerable value to be protected, but, at the same time, privacy is the target of investigations â the Agencies must protect privacy but are allowed broad powers to access and use PI intrusively. The research can theorise on the dynamic interaction of these opposing interests and the resulting impact on privacy.

After having studied the oversight tools the Agencies must comply with and given that the Agencies have as their primary consideration the greater interest of law enforcement and national security, solely entrusting the Agencies with safeguarding privacy may be creating a clear conflict of interest. It is difficult to balance the powers of the Agencies and protect privacy under these circumstances. The studies by the authors did not sufficiently dissect how LI generated and exchanged in modern telecommunications networks is accessed under authorisations issued by the Agencies themselves instead of a judge, and how privacy is used as a limit to those very powers, and the clear conflict that arises. The studies proposed can describe the weaknesses of the legal privacy protections for LI, in contrast to the stronger protections for voice and SMS contents, which are as sensitive and as personal as LI (*CAC Determination 2015* [25]; TIA Act 1979 [14] ss 107H, 108(1)).

The review reveals a lack of detailed research in the following areas:

- How LI is generated and exchanged in the IP-mediated LTE network, and how mobile devices are tracked and create precise location estimates, in the context of the exceptions and privacy safeguards introduced after 2015;
- The discretionary powers of the Agencies to use PI and SI to identify inquiries and investigations to pursue, to enforce the law and perform their functions, and to carry out activities related to their functions and purposes (Revised Explanatory Memorandum, 2015 [102], p. 5 [22] â [23]; *CAC Determination 2015* [25]);
- The flexible oversight principles contained in the guidelines that create conflicts between law enforcement and privacy interests for the Agencies (Attorney-Generalâs Guidelines [78] s 13; *CAC Determination 2015* [25]);
- Court precedents about security, investigations, the transparency and review opportunities of the powers of the Agencies, interpreting the discretionary powers of the Agencies to inquire into, pursue and enforce the law; and
- A critical analysis of what is content, and how content is treated under the law versus how LI is treated as metadata, based on how equally sensitive LI and metadata are, given how modern LTE networks and BLD operate.

The Agencies are required to comply with various privacy standards, but these standards are as vague as the broad powers of the Agencies (Attorney-Generalâs Guidelines [78] s 13; Privacy Act [10] Schedule 1 Part 2 3.1.). This creates a framework that makes it difficult to challenge the powers of the Agencies at the time of collecting the LI from the Telco. Unlike warrants, where Judges oversee privacy as independent third parties, the Agencies play the role of the judge (Telecommunications (Interception and Access) Regulations, 2017 [103] (Cth) Schedule 1, Form 6). The moment when LI is collected from the Telco is the moment when privacy is at its most vulnerable, and the moment external oversight is appropriately required but clearly lacking.

Subject to a detailed study, the framework appears to be designed in the following manner:

- The inquiry and investigative powers are broad;
- the restrictions are more enabling than restrictive (Attorney-Generalâs Guidelines [78]);
- the collection procedures are not transparent (*CAC Determination 2015* Part 3 [25]; TIA Act 1979 [14] ss 107H, 108(1));
- the standards to collect and use LI are high and based on the âreasonable manâ test but at the same time are subject to the sole discretion of the Agencies, with no avenue to challenge whether the test was complied with objectively (*CAC Determination 2015* Part 3 [25]; TIA Act 1979 [14] ss 107H, 108(1), Parts 1â3);
- the Telco is not required to follow the privacy standards of reasonable, necessary, justifiable and proportional when disclosing LI to the Agencies, whereas the Agencies are required to do so when requesting the LI (TIA Act 1979 [14] ss 175-184; TA 1997 [15] ss 275A, 276, 313(3), 313(4), 3131(7); *CAC Determination 2015* [25]); and

- the Agencies are not required to follow the privacy standards of reasonable, necessary, justifiable and proportional when collecting LI from the Telco in respect of all individuals (*CAC Determination 2015* [25]*;* the *Samsonidis* case [21]). As a result, the privacy tests are selectively applied, resulting in potential discriminatory treatment.

The commercial and network maintenance interests of the Telco need to be examined, as well as the indefinite retention period and continued use of the LI, which leaves the LI at the discretion of the Agencies for longer than two years. The Telcoâs discretion to disclose LI voluntarily to the Agencies and the discretion of the Agencies and the Telco to retain LI for any length of time jointly appear to outweigh the privacy interests of the individual in an unfair manner that appears to lead to poor privacy safeguards. This, however, needs to be examined thoroughly. The privacy of the individual is left to the discretion of the Agencies and the Telco. This framework appears to lead to the inadequate protection of privacy, and leaves privacy vulnerable as a check on the powers of the Agencies. Access to LI should be implemented fairly. It may be reasonable to agree that LI should be granted similar legislative privacy protections as voice and SMS communications.

Conclusion

This article was a review of existing literature with comments about the adequacy of the body of work that has been undertaken to date. The paper reviewed the inadequacy of existing literature to holistically analyse the impact on privacy after the 2015 introduction of the telecommunications data retention and disclosure framework, based on how the IP-mediated LTE network generates, stores and shares LI and how this LI is analysed to reveal SI and PI, using BLD analytics, and in relation to existing governance tools. The paper highlighted how the powers of the Agencies to access and use telecommunications data appear not to adequately protect privacy before 2015 and do not do so after 2015, but one must accept that this conclusion requires a contemporary and detailed study to confirm the preliminary arguments.

Acknowledgements

Thanks to UNSW, SEIT (ACCS, UNSW Law); and the D2D CRC LTD, whose financial support made this research possible.

References

ACMA. 2017a. Site Location Map <https://web.acma.gov.au/rrl/site_proximity.main_page>

ACMA. 2017b. *Communications report 2016â17*

Australian Security Intelligence Organization (ASIO) Act 1979 (Cth)

Attorney-Generalâs Department. 2015. Submission No 27 to the Parliamentary Joint Committee on Intelligence and Security (PJCIS), *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, 16 January 2015

Attorney-Generalâs Department. 2016. âAttorney-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)â, June (Attorney-General's Guidelines). http://www.asio.gov.au/About-ASIO/Oversight-and-Accountability/Attorney-General-Guidelines.html [104]

Australian Privacy Commissioner. 2015. Submission No 92 to the Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, January 2015

Australian Attorney-Generalâs Department. 2012. âEquipping Australia against Emerging and Evolving Threatsâ, *Discussion Paper*, July 2012

Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd. 2001. HCA 63 (the Lenah Game case)

Australia & New Zealand Bank v Ryan. 1968. 88 WN (Pt I) (NSW) 368

Barclays Bank Plc. (Trading as Barclaycard) v Taylor [l989] 1 1 WLR 1066

Battersby, L. 2012. âTelstra offers signal boost â at a priceâ,*Sydney Morning Herald* (online), 6 July 2012 http://www.smh.com.au/business/telstra-offers-signal-boost--at-a-price-2012â0706-21l5f.html [105]

Bellovin, SM; Blaze, M; Landau, S; Pell, SK. 2016. âItâs Too Complicated: The Technological Implications of IP-Based Communications on Content/Non-Content Distinctions and the Third Party Doctrineâ. *Harvard Journal of Law & Technology,* 30(1), 1-101

Bloch V; Wark V (eds). 2015. âAustralian Internet Data Collection â Are We Fighting to Protect Privacy Which Is Already Lostâ. *Communications Law Bulletin,* 34(2), 23-27

Bramwell, O. 2012. *A delicate balancing act: data protection, individual privacy & the right to be forgotten: tackling data retention in the digital age* (LLB Thesis). Melbourne, Monash University

Burgess, M. 2015. âWhy new âmetadataâ laws are vital for policeâ.*Police Association (Victoria) Journal,* 81(5), May 2015, pp 16â17. https://search.informit.com.au/documentâSummary;dn=340074488849139;res=IELAPA [106]

Carona, X; Bosua, R; Maynard, SB; Ahmad, A. 2016. âThe Internet of Things (IoT) and its impact on individual privacy: An Australian perspectiveâ. *Computer Law & Security Review,* 32(1), 4â15. http://dx.doi.org/10.1016/j.clsr.2015.12.001 [107]

Carpenter v. United States (Supreme Court of the United States of America, No. 16-402, 22 June 2018) IV 18. https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

Christoj v Barclays Bank. 2000. 1 WLR 937

Chan, J; Moses, LB. 2017. âMaking Sense of Big Data for Securityâ,*The British Journal of Criminology,* 57(2), 299-319

Clarke, R. 2015. âData retention as mass surveillance: The need for an evaluative frameworkâ. *International Data Privacy Law,* 5(2), pp 121â132. http://dx.doi.org/10.1093/idpl/ipu036 [108]

Clarke, R. 2016. âPrivacy Impact Assessments as a Control Mechanism for Australian National Security Initiativesâ. *Computer Law & Security Review,* 32, pp 403â418.

Commonwealth, Parliamentary Debates, Senate, 25 March 2016, 2294 (George Brandis MP)

Communications Access Coordinatorâs (CAC) *Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2015 (Cth) (at 9 October 2015) [CAC Determination 2015]*

Davies, D. 2001. âUnprincipled privacy: Why the foundations of data protection are failing usâ,*UNSW Law Journal,* 24(1), 284-289

Day v Commissioner, Australian Federal Police. 2000. FCA 1272 (11 September 2000) (the *Day* case)

Department of Parliamentary Services (Cth), Bills Digest, No. 10 of 2007-08, 3 August 2007

D*igital Rights Ireland Ltd v Minister for Communications,Marine and Natural Resources* (C-293/12 and C-594/12) [2014] ECJ

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006

ETSI. 2016a. âDigital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Functional stage 2 description of Location Services (LCS)â, (3GPP TS 23.271 version 13.0.0 Release 13)

ETSI. 2017a. âLTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Stage 2 functional specification of User Equipment (UE) positioning in E-UTRANâ, 2017, (3GPP TS 36.305 version 14.2.0 Release 14)

ETSI. 2017b. âLawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained dataâ, 2014, TS 102 657 V1.15.1 (2014-08)

ETSI. 2017c. âLTE; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2â, 2017

ETSI. 2017d. âLTE; Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol A (LPPa)â

ETSI. 2017e. âLTE; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)â

ETSI. 2017f. âDigital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Network architectureâ, 2017, (3GPP TS 23.002 version 14.1.0 Release 14) ETSI TS 123 002 V14.1.0 (2017-05)

ETSI. 2017g. âUniversal Mobile Telecommunications System (UMTS); LTE; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocolâ

Evidence to PJCIS, 30 January 2015, 48 (Malcolm Lanyon, Assistant Commissioner Commander, Special Services Group, New South Wales Police Force)

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)

Farrell; Secretary, Department of Immigration and Border Protection (Freedom of information)[2017] AATA 409 (31 March 2017) (the *Farrel* case)

Fair, P. 2015) âMandatory Data Retention: Overview and Issues Citationâ. *Inhouse Counsel*, 19(8), 110

Fernandes, F; Sivaraman, V. 2015. âItâs only the beginning: Metadata Retention laws and the Internet of Thingsâ. *Australian Journal of Telecommunications and the Digital Economy*, 3(3), 47â57. http://dx.doi.org/10.18080/ajtde.v3n3.21 [109]

Federal Commissioner of Taxation v Australia & New Zealand Banking Group (1979) 143 CLR 499

Germano, A. 2010. âThe Impact of Femtocells on Next Generation LTE Mobile Networksâ, (PowerPoint Presentation at the FemtoForum) 1â30. ftp://www.3gpp.org/Informationâ/presentations/presentations_2010/2010_05_Moscow/Femto_Forum_Germano.pdf [110]

Golder, B; Williams, G. 2006. âBalancing national security and human rights: Assessing the legal response of common law nations to the threat of terrorismâ. *Journal of Comparative Policy Analysis: Research and Practice*, 8(1), 43-62.

Human & Constitutional Rights Resource Page. 2018 http://www.hrcr.org/safricaâ/privacy/austr_law.html [111]

iiNet. 2015. Law enforcement agencies contact https://www.iinet.net.au/aboutâ/legal/law.html [112]

IETF. 2007. âRequest for Comments: 4960 Stream Control Transmission Protocolâ.

IETF. 1981a. âRFC. Transmission Control Protocol DARPA Internet Program Protocol Specificationâ

IETF. 1981b. âRFC 791. Internet Protocol DARPA Internet Program Protocol Specificationâ

InspectorâGeneral of Intelligence and Security Act 1986 (Cth) (IGIS Act)

Jaffarie v Director General of Security[2014] FCAFC 102 (18 August 2014)

Johnston, A. 2017. âPrivacy law: Data, metadata and personal information: A landmark ruling from the federal courtâ. *Law Society of NSW Journal,*31 (March), 82-83.

Jones, DM. 2016. âIntelligence and the management of national security: the post 9/11 evolution of an Australian National Security Communityâ. *Intelligence and National Security*, 33(1), 1â20.

Kozierok, C. 2005. The TCP/IP Guide in the TCP/IP Guide. http://www.tcpipguide.âcom/free/t_MessagesPacketsFramesDatagramsandCells-2.htm [113]

Lachmayer, K; Witzleb, N. 2014. âThe Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspectiveâ. *UNSW Law Journal,* 37(2), 748-783

Laster, D. 1989. 'Breaches of Confidence and of Privacy by Misuse of Confidential Information'.*Otago Law Review* 31, 424

Legal and Constitutional Affairs References Committee (LCARC), Parliament of Australia, *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979*, (2015)

Leonard, P. 2015a. âThe Metadata Retention Debate Rages Onâ.*Internet Law Bulletin,* 18(1) 17. https://www.gtlaw.com.au/sites/default/files/The-Metadata-Retention-Debate-rages-on.âpdf [114]

Leonard, P. 2015b. âInternet Data Retention in Australia: New Controversies and Complexitiesâ.*Privacy Law Bulletin* 2, 12(1) (Lexis Nexis, online)

Leonard, P. 2015c. âMandatory Internet Data Retention in Australia â Looking the horse in the mouth after it has boltedâ. https://www.gtlaw.com.au/sites/default/files/Mandatory-Internet-Data-Retention-in-Australia_0.pdf [115]

Loyd v Freshjeld (1826) 2 Car & P 325; 172 ER 147

Letter from the Attorney General, George Brandis to Hon Philip Ruddock MP, Chair of the PJCIS, 9 February 2016 cited in PJCHR, 25 February 2016

Maurushat, A. 2016. âBD use by law enforcement and intelligence in the national security space: Perceived benefits, risks and challengesâ. *Media and Arts Law Review,* 21(3), 1â27.

Mayer, J; Mutchler P; Mitchell, JC. 2016. âEvaluating the privacy properties of telephone metadataâ. *Proceedings of the National Academy of Sciences of the United States of America*, 113(20), pp. 5536â5541

Michael, K; Clarke, R. 2012. âLocation privacy under dire threat as uberveillance stalks the streetsâ. *Precedent,* 108, 24â29.

Moses, LB; Chan, J. 2014. âUsing Big Data for Legal and Law Enforcement Decisions: Testing the New Toolsâ. *UNSW Law Journal,* 37(2), 643-678

Nicholson, N; Redlich, H. 2015. âBig Data, Metadata and Personal Data - How Does the Privacy Act Regulate Metadata?â *Privacy Law Bulletin,* 12(8), 215 (online)

Nohrborg, M. 2017. LTE, 3GPP. http://www.3gpp.org/technologies/keywords-acronyms/98-lte

Office of Australian Information Commissioner (OAIC, January 2015, Submission No 92 to the Parliamentary Joint Committee on Intelligence and Security, Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, January 2015

Parliamentary Joint Committee on Human Rights (PJCHR). 2014. Parliament of Australia, Fifteenth Report of the 44thParliament

Parliamentary Joint Committee on Intelligence and Security (PJCIS). 2015. Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth)

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

Privacy Act 1988 (Cth)

Revised Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Cth)

Rodrick, S. 2009) âAccessing telecommunications data for national security and law enforcement purposesâ. *Federal Law Review,* 37, 391.

Rix, M. 2013. âSecurity without secrecy? Counter-terrorism, ASIO and access to informationâ, pp. 240-263 in Baldino, D. (Ed), *Spooked: the truth about intelligence in Australia* Sydney, Australia: NewSouth Publishing.

Rix, M. 2014. âWhat is the meaning and what is the use of âmetadata retentionâ?â*The Conversation* (online) 26 August 2014. https://theconversation.com/what-is-the-meaning-and-what-is-the-use-of-metadata-retention-30350 [116]

Robertson v Canadian Imperial Bank of Commerce [l9941 1 WLR 1493

Roach, K. 2011. *The 9/11 Effect: Comparative Counter-Terrorism*. Cambridge: Cambridge University Press.

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

Sarre, R. 2017. âMetadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australiaâ. *Asian Journal of Criminology,* 12(3) pp. 167â179

Selvadurai, N; Gillies, P; Islam, R. 2009. âMaintaining an effective legislative framework for telecommunications interception in Australiaâ. *Criminal Law Journal*, 33(1), 34â44

Selvadurai, N; Kisswani, N; Khalaileh, Y. 2016. âThe proportionality principle in telecomÂmunications interception and access law in an environment of heightened security and technological convergenceâ. *Information & Communications Technology Law*, 25(3), 229-246. doi:10.1080/13600834.2016.1230925

Selvadurai, N. 2017. âThe retention of telecommunications metadata: A necessary national security initiative or a disproportionate interference with personal privacy?â *Computer and Telecommunications Law Review*, 23(2), pp 35â41.

Senate Legal and Constitutional Affairs References Committee (SLCARC), Parliament of Australia, *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979*(2015)

Shanapinda, S. 2017. âRetention and disclosure of location information and location identifiers OTT content and communication servicesâ. *Australian Journal of Telecommunications and the Digital Economy*, 4(4), 251-279. https://doi.org/10.18080/ajtde.v4n4.68 [117]

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 â An Australian story*, (PhD Thesis). UNSW Canberra University (unpublished)

Smith, GJD; Moses, B; and Chan, J. 2017. âThe Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approachâ. *The British Journal of Criminology,* 57(2), pp 259â274.

SSHD v Watson & Others Secretary of State for The Home Department and Tom Watson MP and others [2018] EWCA Civ 70 (the *Watson case)*

Svantesson, DJB. 2012. âSystematic government access to private-sector data in Australiaâ.*International Data Privacy Law*, 2(4), 268â276.

Taylor, G. 2000. âWhy is there no Common Law Right of Privacy?â*Monash University Law Review*, 10, 26(2) 235.

Telstra Corporation Limited and Privacy Commissioner [2015] AATA 991 (18 December 2015)

Telecommunications (Interception and Access) (Data Retention) Amendment Act 2015 (Cth) (*Data Retention Act*)

Telecommunications Interception Legislation Amendment (TILA) Act 2002 (Cth)

Telecommunications (Interception and Access) Regulations 2017 (Cth)

Telstra. 2015. Submission No 112 to the Parliamentary Joint Committee on Intelligence and Security, (PJCIS) *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, January

Telecommunications (Interception and Access) Act 1979 (Cth)

Telecommunications Act 1997 (Cth)

Tournier v National Provincial & Union Bank of England [l9241 1 KB 461

USA FREEDOM Act 2015, 114â23 H.R.2048

Victoria Park Racing and Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479 (the Victoria Park case)

Vodafone Hutchinson Australia. 2017. âPrivacy, 2017â. https://www.vodafone.com.auâ/about/legal/privacy

Williams, G and Hardy, K. 2014. âNational security reforms stage one: Intelligence gathering and secrecyâ [online]. LSJ: *Law Society of NSW Journal*, No. 6, Nov 2014: 68-69. Availability: https://search.informit.com.au/documentSummary;dn=785911277868564;res=IELAPA [118]

Williams, G. 2016. âThe Legal Assault on Australian Democracyâ.*QUT Law Review*, 16(2), 19-41.

Williams, G. 2005. âBalancing National Security and Human Rights: Lessons from Australiaâ. *Borderlands e-Journal*, 4(1) http://www.borderlands.net.au/vol4no1_2005/williams_âbalancing.htm [119]

Winterton Constructions v Hambros (1992) 39 FCR 97, 114-15

Zwolenski, M; Weatherill, L. 2014. âThe digital universe: Rich data and the increasing value of the internet of thingsâ. *Australian Journal of Telecommunications and the Digital Economy,* 2(3), 41â49. http://doi.org/10.7790/ajtde.v2n2.47 [120]

Endnotes

[i] The *USA FREEDOM Act* 2015 was passed to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes. Sec. 101 defines "call detail record" as session identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call. Excludes from such definition: (1) the contents of any communication; (2) the name, address, or financial information of a subscriber or customer; or (3) cell site location or global positioning system information.
[ii] [121] Â© 2017.3GPPâ¢ TSs and TRs are the property of ARIB, ATIS, CCSA, ETSI, TSDSI, TTA and TTC who jointly own the copyright in them. They are subject to further modifications and are therefore provided to you âas isâ for information purposes only. Further use is strictly prohibited.
[iii] [122] 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 l) (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.
[iv] [123] Yelp, Google Places and Facebook.
[v] [124] Application Programming Interface.
[vi] [125] Section 275A was added by the *Communications Legislation Amendment (Content Services) Act 2007* (Cth). Date of Assent: 20 Jul 2007 https://www.legislation.gov.au/Details/C2007A00124 [126].

Article PDF:
167-article_text-1744-1-11-20190116.pdf [127]

Copyright notice:

Copyright is held by the Authors subject to the Journal Copyright notice. [128]

Cite this article as:

Stanley Shanapinda. 2018. *Privacy of Location Information* ajtde, Vol 6, No 4, Article 167. http://doi.org/10.18080/ajtde.v6n4.167 [129]. Published by Telecommunications Association Inc. ABN 34 732 327 053. https://telsoc.org [130]

Metadata retention [131] | Law Enforcement and Privacy [132] | metadata disclosure [133] | privacy [134]

Law enforcement [135] | LTE [136] | Location information [137] | National security [138]

Source URL:https://telsoc.org/journal/ajtde-v6-n4/a167
Links
[1] https://telsoc.org/journal/author/stanley-shanapinda [2] https://telsoc.org/journal/ajtde-v6-n4 [3] https://www.addtoany.com/share#url=https%3A%2F%2Ftelsoc.org%2Fjournal%2Fajtde-v6-n4%2Fa167&title=Privacy%20of%20Location%20Information [4] https://telsoc.org/printpdf/2329?rate=zMX8CH4elXOw6OHyfe3k8GYiSNNSjLzyFvKo3c4aUDA [5] https://telsoc.org/journal/ajtde-v6-n4/a167#SSHD [6] https://telsoc.org/journal/ajtde-v6-n4/a167#DigitalRightsCaseLOCATION [7] https://telsoc.org/journal/ajtde-v6-n4/a167#USAFreedomLOCATION [8] https://telsoc.org/journal/ajtde-v6-n4/a167#CarpenterCaseLOCATION [9] https://telsoc.org/journal/ajtde-v6-n4/a167#_edn1 [10] https://telsoc.org/journal/ajtde-v6-n4/a167#PrivacyAct1988LOCATION [11] https://telsoc.org/journal/ajtde-v6-n4/a167#DataRetentionAct2015LOCATION [12] https://telsoc.org/journal/ajtde-v6-n4/a167#AGDSubmission2015LOCATION [13] https://telsoc.org/journal/ajtde-v6-n4/a167#TelstraSubmissionLOCATION [14] https://telsoc.org/journal/ajtde-v6-n4/a167#TIAAct1979LOCATION [15] https://telsoc.org/journal/ajtde-v6-n4/a167#TAAct1997LOCATION [16] https://telsoc.org/journal/ajtde-v6-n4/a167#TelstraCaseLOCATION [17] https://telsoc.org/journal/ajtde-v6-n4/a167#PrivacyCommissionerCaseLOCATION [18] https://telsoc.org/journal/ajtde-v6-n4/a167#FarrellCaseLOCATION [19] https://telsoc.org/journal/ajtde-v6-n4/a167#JaffarieCaseLOCATION [20] https://telsoc.org/journal/ajtde-v6-n4/a167#DayCaseLOCATION [21] https://telsoc.org/journal/ajtde-v6-n4/a167#SamsonidisCaseLOCATION [22] https://telsoc.org/journal/ajtde-v6-n4/a167#Leonard2015c [23] https://telsoc.org/journal/ajtde-v6-n4/a167#ETSI2017aLOCATION [24] https://telsoc.org/journal/ajtde-v6-n4/a167#Bellovin_2016 [25] https://telsoc.org/journal/ajtde-v6-n4/a167#CACDetermination2015LOCATION [26] https://telsoc.org/journal/ajtde-v6-n4/a167#BlochWark2015LOCATION [27] https://telsoc.org/journal/ajtde-v6-n4/a167#IETF2007LOCATION [28] https://telsoc.org/journal/ajtde-v6-n4/a167#ETSI2017dLOCATION [29] https://telsoc.org/journal/ajtde-v6-n4/a167#ETSI2017eLOCATION [30] https://telsoc.org/journal/ajtde-v6-n4/a167#ETSI2016aLOCATION [31] https://telsoc.org/journal/ajtde-v6-n4/a167#ETSI2017fLOCATION [32] https://telsoc.org/sites/default/files/images/tja/167figure1.jpg [33] https://telsoc.org/journal/ajtde-v6-n4/a167#_edn2 [34] https://telsoc.org/journal/ajtde-v6-n4/a167#Kozierok2005 [35] https://telsoc.org/journal/ajtde-v6-n4/a167#IETF1981aLOCATION [36] https://telsoc.org/journal/ajtde-v6-n4/a167#IETF1981bLOCATION [37] https://telsoc.org/journal/ajtde-v6-n4/a167#CommnwealthParlDebatesSenate25MaLOCATION [38] https://telsoc.org/journal/ajtde-v6-n4/a167#TAAct1997 [39] https://telsoc.org/journal/ajtde-v6-n4/a167#LCARC2015LOCATION [40] https://telsoc.org/journal/ajtde-v6-n4/a167#Leonard2015cLOCATION [41] https://telsoc.org/journal/ajtde-v6-n4/a167#DepartmentParl2007LOCATION [42] https://telsoc.org/sites/default/files/images/tja/167figure2.jpg [43] https://telsoc.org/journal/ajtde-v6-n4/a167#EvidencetoPJCIS2015LOCATION [44] https://telsoc.org/journal/ajtde-v6-n4/a167#Nohrborg2017LOCATION [45] https://telsoc.org/journal/ajtde-v6-n4/a167#ETSI2017gLOCATION [46] https://telsoc.org/journal/ajtde-v6-n4/a167#Germano2010LOCATION [47] https://telsoc.org/journal/ajtde-v6-n4/a167#ETSI2017bLOCATION [48] https://telsoc.org/journal/ajtde-v6-n4/a167#ETSI2017cLOCATION [49] https://telsoc.org/journal/ajtde-v6-n4/a167#SelvaduraiGilliesIslam2009LOCATION [50] https://telsoc.org/journal/ajtde-v6-n4/a167#MichaelClarke2012LOCATION [51] https://telsoc.org/journal/ajtde-v6-n4/a167#FernandesSivaraman2015LOCATION [52] https://telsoc.org/journal/ajtde-v6-n4/a167#ZwolenskiWeatherill2014LOCATION [53] https://telsoc.org/journal/ajtde-v6-n4/a167#CaronaBosuaMaynardAhmad2016LOCATION [54] https://telsoc.org/journal/ajtde-v6-n4/a167#Taylor_2000 [55] https://telsoc.org/journal/ajtde-v6-n4/a167#HumanConstitutionalRightsResourcLOCATION [56] https://telsoc.org/journal/ajtde-v6-n4/a167#VictoriaParkcase193758CLR479 [57] https://telsoc.org/journal/ajtde-v6-n4/a167#LenahGameMeatscase2001LOCATION [58] https://telsoc.org/journal/ajtde-v6-n4/a167#_edn3 [59] https://telsoc.org/journal/ajtde-v6-n4/a167#VodafoneHutchAustraliaPri2017LOCATION [60] https://telsoc.org/journal/ajtde-v6-n4/a167#LachmayerWitzleb2014LOCATION [61] https://telsoc.org/journal/ajtde-v6-n4/a167#RoachK2011LOCATION [62] https://telsoc.org/journal/ajtde-v6-n4/a167#Davies2001LOCATION [63] https://telsoc.org/journal/ajtde-v6-n4/a167#Williams2005LOCATION [64] https://telsoc.org/journal/ajtde-v6-n4/a167#GolderWilliams2006LOCATION [65] https://telsoc.org/journal/ajtde-v6-n4/a167#BramwellThesis2012LOCATION [66] https://telsoc.org/journal/ajtde-v6-n4/a167#NicholsonRedlich2015LOCATION [67] https://telsoc.org/journal/ajtde-v6-n4/a167#Leonard2015aLOCATION [68] https://telsoc.org/journal/ajtde-v6-n4/a167#Leonard2015bLOCATION [69] https://telsoc.org/journal/ajtde-v6-n4/a167#Fair2015LOCATION [70] https://telsoc.org/journal/ajtde-v6-n4/a167#Rodrick2009LOCATION [71] https://telsoc.org/journal/ajtde-v6-n4/a167#ShanapindaSRetentionandDisclosureOTT2017 [72] https://telsoc.org/journal/ajtde-v6-n4/a167#Selvadurai2017LOCATION [73] https://telsoc.org/journal/ajtde-v6-n4/a167#Directive2006LOCATION [74] https://telsoc.org/journal/ajtde-v6-n4/a167#Clarke2015LOCATION [75] https://telsoc.org/journal/ajtde-v6-n4/a167#Clarke2016LOCATION [76] https://telsoc.org/journal/ajtde-v6-n4/a167#SelvaduraiKisswaniKhalaileh2016LOCATION [77] https://telsoc.org/journal/ajtde-v6-n4/a167#AGDEquippingAustraliaLOCATION [78] https://telsoc.org/journal/ajtde-v6-n4/a167#AttorneyGeneralsGuidelinesLOCATION [79] https://telsoc.org/journal/ajtde-v6-n4/a167#WilliamsHardy_2014 [80] https://telsoc.org/journal/ajtde-v6-n4/a167#Rix2013LOCATION [81] https://telsoc.org/journal/ajtde-v6-n4/a167#Sarre2017LOCATION [82] https://telsoc.org/journal/ajtde-v6-n4/a167#LetterFromAG9Febr2016LOCATION [83] https://telsoc.org/journal/ajtde-v6-n4/a167#IGIS_1986 [84] https://telsoc.org/journal/ajtde-v6-n4/a167#Burgess2015LOCATION [85] https://telsoc.org/journal/ajtde-v6-n4/a167#Svantesson2012LOCATION [86] https://telsoc.org/journal/ajtde-v6-n4/a167#Jones2016LOCATION [87] https://telsoc.org/journal/ajtde-v6-n4/a167#ASIOAct1979LOCATION [88] https://telsoc.org/journal/ajtde-v6-n4/a167#MayerMutchlerMitchell2016LOCATION [89] https://telsoc.org/journal/ajtde-v6-n4/a167#_edn4 [90] https://telsoc.org/journal/ajtde-v6-n4/a167#_edn5 [91] https://telsoc.org/journal/ajtde-v6-

n4/a167#Battersby2012LOCATION [92] https://telsoc.org/journal/ajtde-v6-n4/a167#ACMA2017LOCATION [93] https://telsoc.org/journal/ajtde-v6-n4/a167#Johnston2017LOCATION [94] https://telsoc.org/journal/ajtde-v6-n4/a167#iiNET2015LOCATION [95] https://telsoc.org/journal/ajtde-v6-n4/a167#MosesChan2014LOCATION [96] https://telsoc.org/journal/ajtde-v6-n4/a167#ChanMoses2017LOCATION [97] https://telsoc.org/journal/ajtde-v6-n4/a167#SmithMosesChanLOCATION [98] https://telsoc.org/journal/ajtde-v6-n4/a167#Maurushat2016LOCATION [99] https://telsoc.org/journal/ajtde-v6-n4/a167#PJCIS2015LOCATION [100] https://telsoc.org/journal/ajtde-v6-n4/a167#_edn6 [101] https://telsoc.org/journal/ajtde-v6-n4/a167#APCSubmission2015LOCATION [102] https://telsoc.org/journal/ajtde-v6-n4/a167#RevisedExplanatoryMemorandum2015LOCATION [103] https://telsoc.org/journal/ajtde-v6-n4/a167#TIARegulations2017LOCATION [104] http://www.asio.gov.au/About-ASIO/Oversight-and-Accountability/Attorney-General-Guidelines.html [105] http://www.smh.com.au/business/telstra-offers-signal-boost--at-a-price-20120706-21l5f.html [106] https://search.informit.com.au/document%E2%80%8CSummary;dn=340074488849139;res=IELAPA [107] http://dx.doi.org/10.1016/j.clsr.2015.12.001 [108] http://dx.doi.org/10.1093/idpl/ipu036 [109] http://dx.doi.org/10.18080/ajtde.v3n3.21 [110] ftp://www.3gpp.org/Information%E2%80%8C/presentations/presentations_2010/2010_05_Moscow/Femto_Forum_G%20ermano.pdf [111] http://www.hrcr.org/safrica/privacy/austr_law.html [112] https://www.iinet.net.au/about/legal/law.html [113] http://www.tcpipguide.com/free/t_MessagesPacketsFramesDatagramsandCells-2.htm [114] https://www.gtlaw.com.au/sites/default/files/The-Metadata-Retention-Debate-rages-on.pdf [115] https://www.gtlaw.com.au/sites/default/files/Mandatory-Internet-Data-Retention-in-Australia_0.pdf [116] https://theconversation.com/what-is-the-meaning-and-what-is-the-use-of-metadata-retention-30350 [117] https://doi.org/10.18080/ajtde.v4n4.68 [118] https://search.informit.com.au/documentSummary;dn=785911277868564;res=IELAPA [119] http://www.borderlands.net.au/vol4no1_2005/williams_%E2%80%8Cbalancing.htm [120] http://doi.org/10.7790/ajtde.v2n2.47 [121] https://telsoc.org/journal/ajtde-v6-n4/a167#_ednref2 [122] https://telsoc.org/journal/ajtde-v6-n4/a167#_ednref3 [123] https://telsoc.org/journal/ajtde-v6-n4/a167#_ednref4 [124] https://telsoc.org/journal/ajtde-v6-n4/a167#_ednref5 [125] https://telsoc.org/journal/ajtde-v6-n4/a167#_ednref6 [126] https://www.legislation.gov.au/Details/C2007A00124 [127] https://telsoc.org/sites/default/files/tja/pdf/167-article_text-1744-1-11-20190116.pdf [128] https://telsoc.org/copyright [129] http://doi.org/10.18080/ajtde.v6n4.167 [130] https://telsoc.org [131] https://telsoc.org/topics/metadata-retention [132] https://telsoc.org/topics/law-enforcement-and-privacy [133] https://telsoc.org/topics/metadata-disclosure [134] https://telsoc.org/topics/privacy [135] https://telsoc.org/topics/law-enforcement [136] https://telsoc.org/topics/lte [137] https://telsoc.org/topics/location-information [138] https://telsoc.org/topics/national-security