The retention and disclosure of location information and location identifiers

OTT content and communications services

Stanley Shanapinda

University of New South Wales

Abstract: This article describes how Australia's metadata retention and disclosure regime addresses the retention and disclosure of location information and location identifiers by locally licensed telecommunications service providers and those that do not require a licence to operate in Australia. It specifically addresses over the-top-content and communications services. It proposes the three-tier TelCo and the two-tier Content and Communications Service Provider framework in the Service Provider-Retention-Disclosure Obligation Relationship Table, as the lens through which to understand the roles of the various parties. The duty to retain and disclose location information and location identifiers to law enforcement and national security agencies without a judicial warrant are described in contrast to the powers of the agencies to access and use location information from free online social networking services. The law however acts to restrict the retention and thereby the disclosure of location information, in respect of over the-top-content and communications services that are not provided by the licensed or unlicensed telecommunications service provider. The paper argues, the retention limitations in respect of over the-top-content and communications services are undermined by the actions of the agencies to harvest location information and conduct Big Data analytics. Similarly, so does the discretion granted to the telecommunications service provider to retain location information in respect of over the-top-content and communications services provided by a third-party service provider and then to be required to disclose it, without any additional safeguards. The actions of the agencies and the discretion granted to the telecommunications companies undermine privacy protections.

Keywords: Metadata, location information, over-the-top content and communications services, location-based services, law enforcement and national security, privacy, personal information

Introduction

Telecommunications service providers (the TelCo) all over the world are required by laws of various jurisdictions to retain and disclose location information and location identifiers to law enforcement and national security agencies, commonly referred to as metadata. Australia revised its telecommunications metadata retention and disclosure regime (the

http://doi.org/10.18080/ajtde.v4n4.68

Regime) on the 13th of October 2015 ("*TIA Amendment (Data Retention) Act 2015 (Cth)*," item 2).

The Regime imposes diverse legal obligations on the TelCo. These obligations are however dependent on the type of telecommunications services provided and the type of TelCo ("*TIA Act 1979 (Cth)*," Section 187A(1) and (3). This paper dissects the categories of TelCo's and discusses the extent of their role with respect to the retention and disclosure of location information and location identifiers.

The article argues, in areas where the law does not impose a retention obligation, that there is still a mandatory warrantless disclosure obligation attached to the location information, in the event the TelCo happens to possess the location information and location identifiers ("*TIA Act 1979 (Cth)*," Sections 172 - 184) and (Fair, 2016). Additionally, the announcement to collect and analyse location information from social networking websites undermines privacy, data protection and data minimisation, which safeguards can be said to be practically created by excluding OTT content service providers from being regulated under the Regime. There appears to be no alternative formal regime under which these service providers are regulated.

The paper firstly discusses the literature that relates to location-based services (LBS) and over-the-top (OTT) content and communications services. It then describes how the LoCation Services (LCS) functionality operates in relation to OTT content and communications services, which are LBS. In doing so, it sketches the technical background, prior to discussing the legal obligations and policy implications. This is in turn contrasted against the legal nature of the TelCo. The corresponding exceptions to the role of the TelCo are then outlined. The impact of the policy positions on privacy are critically assessed against the safeguards bestowed by the law.

Related works

Soon after the *TIA Act 1979 (Cth)* was amended in 2008, Nicholls and Rowland criticised access to prospective location information by law enforcement and national security agencies without a judicial warrant (Nicholls & Rowland, 2008b). Nicholls and Rowland outlined the legal obscurities regarding what they called communications metadata. They described the Regime as uncertain. This uncertainty referred to the lack of a definition of telecommunications data. Less detail was publicly available about the extent and the types of information to be retained and the limitations placed on the TelCo about the types of location information to retain and in respect of which types of services and communications. The legal position was largely uncertain, as identified by Nicholls & Rowland (2008b), but it has since been revised.

http://doi.org/10.18080/ajtde.v4n4.68

Rodrick (2009) addressed the privacy impacts of mobile phone data location, arguing the Regime, as it was then, should be reconfigured to afford better privacy protection to the individual. The peculiarities of OTT content and communications services and the various TelCo were however not considered.

Abbas et al (2013) sketched and proposed a LBS regulatory framework in the Australian social context. Although the authors recognised that LBS are bound by surveillance, telecommunications, privacy and national security legislation, they concluded the framework existing at the time did not adequately address location information. They also concluded that the 2013 framework inadequately addressed the themes and challenges in the conceptual framework. They concluded:

> A number of issues inevitably emerge upon closer examination of the current LBS regulatory framework in Australia. With regards to privacy legislation, it was noted that (location) information derived from LBS solutions might or might not be personal information and is unlikely to be sensitive personal information. The Privacy Act may not cover the data. Regarding Australian telecommunications legislation, location information may not specifically be classed 'telecommunications data' in all circumstances. The location-dependent carriage service introduces ambiguity regarding definitions (Abbas et al., 2013, p. 585).

Furthermore, in 2013, Abbas et al. (2013) found that the framework does not account for location information generated by LBS, due to its technology-neutral approach. Recent legal developments have since specifically addressed location information in respect of LBS ("*TIA Act 1979 (Cth)*," Section 187A(4)(c).

Michael & Michael (2011) discussed the social and behavioural implications of LBS in the current global "uberveillance" environment and the risks to privacy. They stated that the way forward regarding the social implications of LBS may be to see it play out in a court of law or to introduce legislation to curb potential harm. Michael & Michael (2011) however cautioned that the right balance should be struck by such regulatory measures so as not to stifle the development of the technology. The Regime has undergone major changes since 2008 and 2011. The latest changes were effected in mid-October 2015.

Clarke & Wigan (2011) described the generic threat to privacy posed by location-based systems, without specifically undertaking a study regarding LBS offered by the Australian TelCo and foreign OTT content and communications service providers (Clarke & Wigan, 2011). The paper investigated the political threats in 2011 and proposed controls and protections. This was four years prior to the Regime being revised and not due to the privacy

http://doi.org/10.18080/ajtde.v4n4.68

threats posed within the legal and policy context of the 2015 revised Regime. In any event, Clarke and Wigan only considered traffic administration, traffic law enforcement, public safety and criminal law enforcement.

Cuijpers & Pekárek (2011) discussed the regulation of LBS in the EU. They identified a particular challenge posed by the non-identifiability and non-traceability of the sources of location information in LBS. This paper describes how the Australian Regime addresses the issues related to non-identifiability and non-traceability.

Gibson (2004, p. 17) defines open source intelligence (OSINT) as information that is legally available and that is in the public domain. Bell & Congram (2014, p. 58) identify OSINT as available on the Internet and accessed by law enforcement agencies. They state that OSINT however poses legal issues, but fail to indicate or speculate about these legal challenges.

Li (2015) did not address retention obligations of OTT content and communications service providers. Instead, Li proposed OTT regulation for universal service purposes.

Existing literature fails to address the recent policy and legal changes in relation to the duties of the TelCo in relation to LBS. These recent changes to policy and law, particularly in relation to the technical specifications of LCS, remain largely un-examined. Recent legal developments therefore require analysis as is undertaken by this article. This paper addresses this shortcoming and proposes the 'Service Provider Retention-Disclosure Obligation Relationship Table' as a framework in terms of which the role of the TelCo may be outlined. This framework addresses privacy protections embedded within it, but also critically highlights how policy decisions erode those same protections, by not regulating OTT content and communications service providers for the purposes of the Regime.

OTT content and communications services

Content and communications services include online information services, online entertainment services (for example, a video-on-demand service or an interactive computer game service), or any other online service ("*Telecommunications Act 1997 (Cth)*," Section 15).

OTT content and communications services runs over the public Internet infrastructure (European Parliament, 2015: p. 22). OTT content and communications services are provided independently of the telecommunications network operator. OTT content and communications services are delivered over a telecommunications network that is not offered by that same network operator. Instead, OTT content and communications services ride on top of the infrastructure service (ACMA, 2015: p. 131). The OTT content and

http://doi.org/10.18080/ajtde.v4n4.68

communications service provider is therefore generally separate from the operator of the IP network that it uses (Li, 2015: p. 30; EuropeanParliament, 2015: p. 22).

Any type of information, entertainment, social media service or application, that is used on a mobile device and that makes use of the devices' approximated geographic location, in name, latitude, longitude or altitude may be considered an LBS (AMTA, 2010: p. 4).

LBS may include mobile location-based advertising, friend location-based services, anonymous chats, dating location-based services and mobile games (AMTA, 2010: p. 5).

The "LoCation Services" functionality used to provide OTT content and communications services

LCS is a standardisation service concept in the telecommunications network. LCS specifies the vital network elements, their functionalities, interfaces and communications messages, for the operation of location positioning in the cellular network (ETSI, 2016b: p. 12 and 13). The LCS functionality is used on relation to OTT content and communications services, making it location-based.

OTT content and communications services are software applications that interact with the LCS server for the purpose of obtaining the location information and location identifiers of a relevant device. For this reason, OTT content and communications services may be referred to as LCS clients (ETSI, 2016b: p. 13). The OTT content and communications service processes the location information and uses it in one way or another. An OTT content and communications service that processes location information and uses it is therefore a location-based application and becomes an LBS (ETSI, 2016b: p. 12 and 13). The positioning feature can be used internally by the telecommunications network, or by the value-added network services, or by the device directly, or through the telecommunications network or by third party services (ETSI, 2016b: p. 20).

Location identifiers are used to identify the device and its estimated location. Location identifiers are the location information about a device, that is related to a given location or is general information. This general information is information about the Global Cell-ID in cellular networks, Line-ID in fixed broadband networks, and the Media Access Control (MAC) address of the Wi-Fi router or mobile device (ETSI, 2016b: p. 13).

The methods used to approximate the position of the device includes using the radio cell coverage, GPS or Assisted-GPS methods based on the Time-Of-Arrival (TOA) algorithm and/or the Time-Difference-Of-Arrival (TDOA) algorithm. The variations include Uplink Time Difference of Arrival (UTDOA), Observed Time Difference Of Arrival (OTDOA) and the Enhanced Observed Time Difference (E-OTD) methods (ETSI, 2016b: p. 14).

http://doi.org/10.18080/ajtde.v4n4.68

Measuring the location is dependent on the design of the network by the TelCo. Most devices, whether idle or active, use the positioning functionality provided by the access network. The radio access network shares the location information with the core network (ETSI, 2016b: p. 20). The positioning functionality may be used for billing purposes by the TelCo for the service the device is connected to (ETSI, 2016b: p. 20). The positioning functionality uses the radio signals to determine the geographic location of the device, which information is forwarded to the OTT content and communications service software application, which is the LCS client, for its use. The radio signals are measured, processed, the estimated location is then produced and delivered to the requesting LCS client (ETSI, 2016b: p. 20).

The LCS functionality is used in both packet-switched and circuit-switched networks. It is technically feasible for various LCS clients to request simultaneous location information in relation to one device (ETSI, 2016b: p. 20).

The IP Multimedia Subsystem (IMS) is used to deliver interactive content, text and voice, which lies at the heart of OTT content and communications services. The IMS Public User Identity (SIP-URI) (ETSI, 2016b: p. 143) and the Mobile Station Integrated Services Data Network Number (MSISDN) (ETSI, 2016b: p. 17) are key device identifiers, that are of interest to the agencies.

The IMS uses the SIP-URI to route LCS service requests for location estimates to the home network of a device. The SIP-URI is used as the public identity of the device on the public Internet (ETSI, 2016b: p. 143). The MSISDN is the number of the device in the IMS. The MSISDN is obtained by the home network of the device from the Home Subscriber Server (HSS) (ETSI, 2016b: p. 27). The MISISDN comprises the Country Code (CC) and the National (significant) mobile number. The National (significant) mobile number in turn comprises the National Destination Code (NDC) and the Subscriber Number (SN) (ETSI, 2016a: p. 22).

The LCS service request is forwarded along with the MSISDN by the home networks' SIP-URI via the interface to the home Gateway Mobile Location Centre (GMLC).

Pre-configured destination addresses or Domain Name Server (DNS) lookups may be used to identify the home network of the device in order to route the information. The MSISDN may be used to get the Internet Protocol (IP) address from the Home Subscriber Register (HLR) or HSS (ETSI, 2016b: p. 143).

Figure 1 below depicts the LCS architecture and demonstrates the LCS functionality in generating and communicating location information and device identifiers, as discussed above.

http://doi.org/10.18080/ajtde.v4n4.68

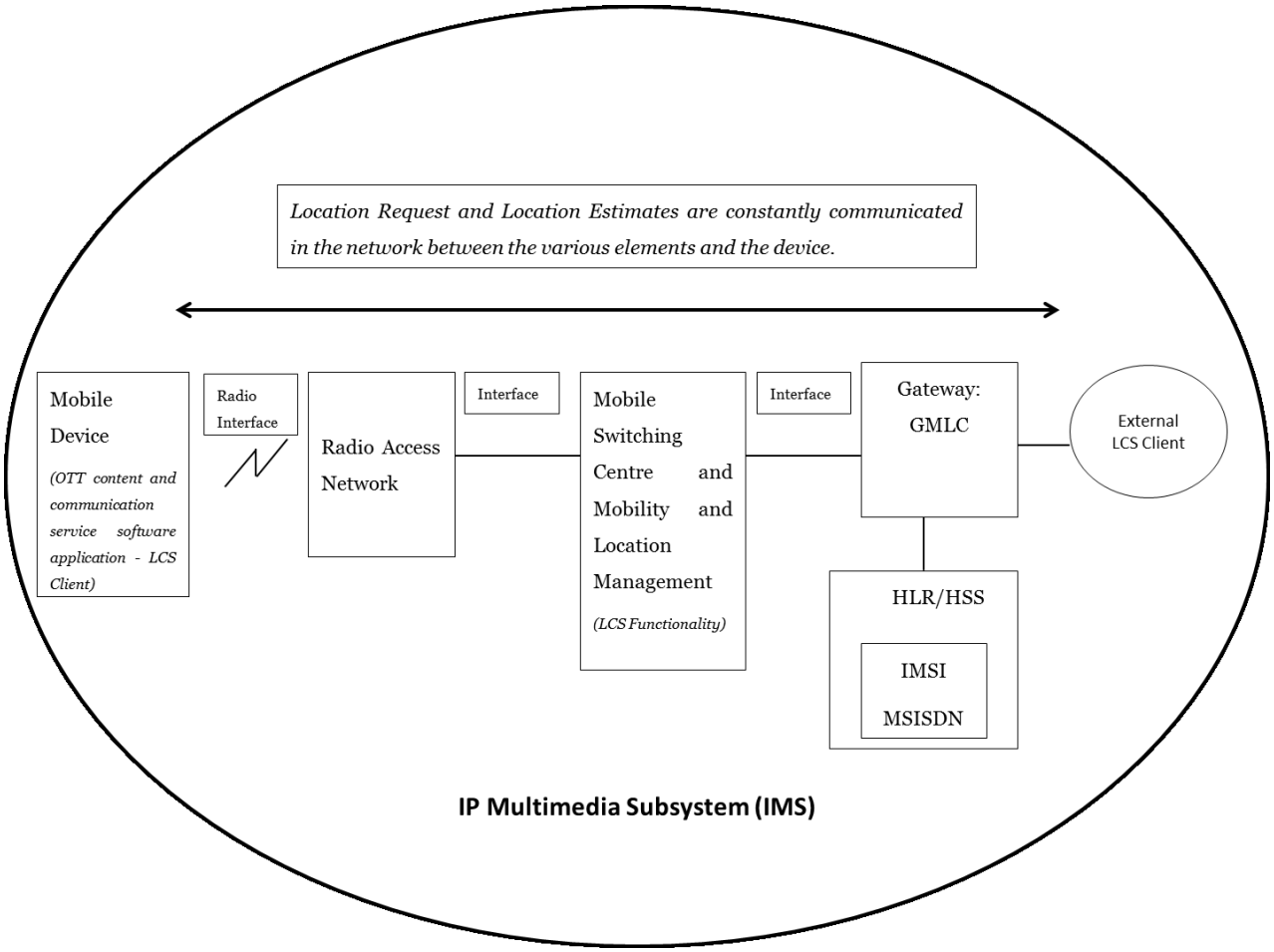

Figure 1: The LCS Functionality and Architecture (Cisco, 2016: p. 299)

The TelCo is therefore required to retain the following types of location information if the TelCo used the information to provide the service:

- International Mobile Subscriber Identity (IMSI),
- International Mobile Equipment Identity (IMEI),
- IP addresses,
- port numbers in respect of OTT content and communications services, which in turn are multi-media communications such as in
  - e-mail,
  - Voice-over-Internet Protocol (VoIP),
  - instant messages or
  - video communication

(*Explanatory Memorandum, 2015*: pp. 47-48).

The degree to which this duty applies to a given TelCo and the OTT content and communications service provider is critically discussed below.

Compelled and voluntary assistance: retention and disclosure

The Australian TelCo is generally required to provide such help as is reasonably necessary to

http://doi.org/10.18080/ajtde.v4n4.68

law enforcement and national security agencies ("*Telecommunications Act 1997 (Cth)*," Section 313(3) and (7)).

The Regime commenced on 13 October 2015 requiring the TelCo to retain location information and location identifiers in respect of the telecommunications services provided and the communications carried ("*TIA Act 1979 (Cth)*," s 187A and 187AA).

The information retained in respect of the telecommunications equipment or a line used in connection with communication, must be retained for a minimum two-year period ("*TIA Act 1979 (Cth)*," Section 187AA(1) items 2, 3, and 6 and Section 187C). The information of the equipment or the line to be retained, is the physical or logical location at the time a communication starts and the location at the time the communication ends ("*TIA Act 1979 (Cth)*," Section 187AA(1) item 6).

The law enforcement and national security agencies authorise the disclosure and the use of the location information and device identifiers by and for themselves, without a judicial warrant being required. The TelCo may voluntarily disclose the information to the agencies for the purpose of law enforcement and national security ("*TIA Act 1979 (Cth)*," Sections 172 - 184).

This retention and disclosure scheme is enforced by means of civil penalty provisions ("*Telecommunications Act 1997 (Cth)*," Schedule 1 Part 31) and (Explanatory Memorandum, 2015: p. 10).

However, location information and location identifiers are only required to be retained in respect of a relevant service. A relevant service is a telecommunications service operated by a carrier or an Internet Service Provider (a TelCo in other words), that carries communications or that enables communications to be carried. This TelCo owns or operates telecommunications infrastructure located in Australia, that enables the relevant telecommunications service ("*TIA Act 1979 (Cth)*," Section 187A(3)). OTT content and communications services such as e-mail, Voice-over-Internet Protocol (VoIP), instant messages or video communication are multi-media communications (Explanatory Memorandum, 2015: pp. 47-48), which may or may not be relevant service, depending on the type of provider. In respect of the retention obligation, there was confusion about which type of TelCo is required to retain metadata in respect of OTT content and communications services (Stanton, 2016).

Infrastructure includes any line or equipment used to facilitate communications across a telecommunications network ("*TIA Act 1979 (Cth)*," Section 5(1), definition of 'infrastructure'). Infrastructure includes website hosting servers and servers hosting services that are provided by OTT content and communications service providers. It also includes

http://doi.org/10.18080/ajtde.v4n4.68

line links and network units (A-G' s Department, 2015: p. 18).

Line links are constituted in three ways: when one line is connected to another line; if two line links are connected; and if the links are connected to the same facility ("*Telecommunications Act 1997 (Cth)*," Section 30). A network unit is formed when a designated radiocommunications facility is used, or is for the use of supplying a carriage service between several points all located in Australia ("*Telecommunications Act 1997 (Cth)*," Subsection 28(1)).

An OTT content and communications service is a telecommunications service that enables communications to be carried. The mandatory telecommunications metadata retention and disclosure obligations generally apply to OTT content and communications services (Explanatory Memorandum, 2015: p. 41), except as stated below.

The TelCo is generally required to retain and disclose the location identifiers such as the IMEI, IMSI, MSISDN (A-G's Department, 2015: pp. 16, 37, 42, 44, 48 and 49) and MAC address (A-G's Department, 2015: pp. 43-44, 49-51). The TelCo is also required to retain the SIP (Session Initiation Protocol) (ETSI, 2016b) address information (A-G's Department, 2015: p. 13).

The three-tier TelCo and the two-tier Content and Communications Service Provider framework

As can be seen from the discussion above, the degree to which the legal obligation to retain and disclose location information and location identifiers is imposed, is largely dependent on the combination of the nature of the telecommunications service and the type of TelCo providing the service. It is also dependent on its distribution and access; who controls and owns the infrastructure; and its configuration ("*TIA Act 1979 (Cth)*," Section 187A(1), (3) and (4).

Three tiers of TelCo may be identified in the telecommunications industry:

- the licensed carrier,
- the CSP and
- OTT content providers.

Whereas the first two are regulated by the Regime, the latter may not be (Fair, 2016). This paper however identifies five role players in the OTT content and communications services provider chain. Their respective nature and how that relates to their retention and disclosure obligations, or not, is discussed in the following sections.

http://doi.org/10.18080/ajtde.v4n4.68

Licensed carrier

The first TelCo is the Australian licensed carrier that owns or operates the telecommunications infrastructure ("*TIA Act 1979 (Cth)*," Section 187A(3)(b)(i) and (c)).

The first tier includes carriers that own network units in Australia, such as microwave or satellite links, but not limited thereto (Fair, 2016).

Carriage Service Provider

The second TelCo is the Australian unlicensed ISP, that owns or operates the telecommunications infrastructure ("*TIA Act 1979 (Cth)*," Section 187A(3)(b)(ii) and (c)). The ISP is the CSP that does not require an ACMA licence to operate (ACMA, 2016).

The second tier includes the CSP. The CSP resells the capacity which is available on the network units of the carriers and therefore does not require a licence to operate (Fair, 2016). The CSP uses a network unit to: '...resell time on a carrier network for phone calls, provide access to the internet (Internet Service Providers) or provide telephone services over the internet (VoIP service providers)' (ACMA, 2016).

The first and second TelCo's may be referred to as the Category A TelCo and the Category B TelCo, respectively.

The Category A TelCo has control over the access and core networks used to provide the OTT content and communications services (European Parliament, 2015: p. 20).

The Category B TelCo may either be a Mobile Virtual Network Operator (MVNO), leasing capacity from the telecommunications network of the aforementioned Category A TelCo (A G's Department, 2015: p. 41), or operate its own network (Fair, 2016).

The Category A or Category B TelCo may provide OTT content and communications services such as Telstra's Data services, BigPond Mobile Services, previously known as Telstra Active or WAP.

BigPond Mobile Services is a mobile video and audio content service (Telstra, 2014: p. 38). In using BigPond Mobile Services, Telstra is licensed to sub-licence these services to its customers. Telstra is licensed to use Blackberry application services and permitted in turn to licence its retail customers to use the service (Telstra, 2014: p. 17).

A TelCo such as Telstra may be classified as a Category A TelCo, in the context of these third party licensed content and communications services. In the event that Telstra develops and licenses its own online content, Telstra would be considered a Category C TelCo, in respect of that OTT content and communications service.

http://doi.org/10.18080/ajtde.v4n4.68

The Category A or B TelCo provides an Internet access service to its individual customers, which customers may access the public Internet to use services such as Gmail or Skype; and use other Invoiced or Free OTT Content and Communications Services.

Over the Top Content Providers

The law appears to create a new category of TelCo that is either a licensed carrier or an unlicensed CSP. The OTT content and communications service is not operated by another person using the relevant service operated by the Category A or Category B TelCo ("*TIA Act 1979 (Cth)*," Section 187(4)(c)).

The law clearly assumes the TelCo itself may be providing an OTT content and communications service without the involvement of a third party, such as Blackberry. This, despite the statements from the Australian Mobile Telecommunications Association (AMTA), and the Australian Communications and Media Authority (ACMA) that OTT content and communications services are provided independent of the TelCo that is the network operator (Li, 2015: p. 30) and (European Parliament, 2015: p. 22).

For example, a carrier grade VoIP service Category A or Category B TelCo is packaging and bundling for its customers, that Category A or Category B TelCo has the responsibility to collect the relevant metadata (Stanton, 2016).

This TelCo may be referred to as the Category C TelCo. Telstra's Mobile Location Manager Service is an OTT content and communications service (Telstra, 2014: pp. 38-40).

Other examples include the Telstra services accessed via its Unstructured Supplementary Service Data (USSD) and Wireless Access Protocol (WAP) for mobile Internet, to ensure the services are interactive. It therefore uses WAP browsers:

- "Whereis", that allows the user to request nearby "points of interest" and the information is send via SMS;
- Local Weather;
- SMS Games;
- MobileFun, a service that you can use to personalise your mobile phone by downloading content including logos, colour wallpaper, animated wallpaper, monophonic and polyphonic ringtones, truetones, real tones, video ringtones, video greetings and SMS picture messages; and
- SMS Alerts from time to time by opting in to receive SMS Alerts via the MobileFun service (Telstra, 2014: pp. 38-40).

http://doi.org/10.18080/ajtde.v4n4.68

Telstra may be operating the service itself, on top of its own IMS network or it may be a licensed service which would classify Telstra as either a Category A or C TelCo with varying retention obligations.

The location of the device is determined by using the cellular network of the TelCo, probably assisted by the GPS and the TOA and TDOA methods (ETSI, 2016b: p. 14). In this instance, the operator may be required to retain the approximate location and location identifiers of the device. These services may use a combination of USSD, WAP (IP network) and the cellular network, to provide the service and to determine the approximate location of the device. The infrastructure that is used is owned and operated by Telstra, as the Telco. Telstra is required to retain the location of the device in its network, when the customer is requesting the content via SMS and the content is delivered via SMS, using the cellular network.

Telstra may then be required to retain and disclose the location information and location identifiers of the device that is accessing and using the OTT content and communications service provided by it. These appear to be the OTT content and communications services Telstra informed the Parliamentary Joint Committee on Intelligence and Security (PJCIS), from which it can extract location information and location identifiers:

> Today we will keep, and, for our purposes, we can tell you, that this phone call was initiated *from this phone* onto *that tower*. After that, if that phone moves around the city, *we do not track what tower it goes to for the purposes of that billing event*. That is why we capture the first thing—*there is a phone call being made*; there is a charge; we need to account for that for billing purposes. Separately in our system, *as we are maintaining a call or allowing a phone to maintain data connectivity if it is talking to a weather app or doing some web browsing, we do know—the system knows; the humans do not know—where that phone is*. So, in that case that Mrs. Hughes gave, if we are looking at where a phone was last seen, *we are able to interrogate our system and, depending on the load of the system, we may well be able to answer that question and say, 'At 2.45 yesterday, we saw that phone for the last time attached to that tower* (Burgess, 2015) (emphasis added).

Other entities

The fourth category of entity that may not necessarily be a TelCo, is an entity that does not own or operate infrastructure in Australia, and does not have a licence to operate in Australia. It is the entity that is the other person that operates the OTT content and communications service using the relevant service operated by the Category A or B TelCo ("*TIA Act 1979 (Cth)*," Section 187(4)(c)). This is the entity that licenses the Category A and B

http://doi.org/10.18080/ajtde.v4n4.68

TelCo to sub-licence its OTT content and communications services to its individual customer. This is a subscription service that is not operated for free, such as Blackberry application services.

This entity may be referred to as the Invoiced Content and Communications Service Provider.

Other providers

The fifth category of entity may not necessarily be a TelCo either. It does not own or operate infrastructure in Australia, and does not have a licence to operate in Australia. It is the entity that is the other person that operates the OTT content and communications service using the relevant service operated by the Category A or B TelCo ("*TIA Act 1979 (Cth)*," Section 187(4)(c)). This is a subscription service that is operated by this third party, but provided for free. This entity may be based locally or internationally. This entity develops the OTT content and communications service as an online service and distributes it over the public Internet for free use without the licensing of the Category A or B TelCo (European Parliament, 2015: p. 20).

This entity may be referred to as the Free Content and Communications Service Provider, such as social networking platforms.

Limitation of information to be retained

There are limitations on the extent to which OTT content and communications services are subject to the obligation to retain and disclose location information and location identifiers.

The first exception

Location information about a telecommunications device, the service or the communication information that states an address to which a communication was sent on the Internet, from a telecommunications device, using an Internet access service provided by the Category A, B or C TelCo; and that was obtained by the Category A, B or C TelCo only as a result of providing the Internet access service, is not required to be retained.

The Category A, B or C TelCo is not required to retain location information and location identifiers about a user's web browsing history ("*TIA Act 1979 (Cth)*," Section 187A(4)(b)). The destination IP addresses, the Uniform Resource Locator (URL) port numbers and other Internet identifiers generated by solely accessing an Internet access service provided by the TelCo are exempted (Explanatory Memorandum, 2015: p. 48).

http://doi.org/10.18080/ajtde.v4n4.68

The policy position appears to be that a URL is considered to be content of a communication, but that in certain instances it may be telecommunications data: 'The provision is required because a URL is in some cases telecommunications data rather than content' (Explanatory Memorandum, 2015: p. 43).

It would appear that for a URL to be disclosed, the law enforcement agencies may not use the warrantless telecommunications metadata authorisation and disclosure process. This is however an issue that requires further investigation and clarification, both from a policy and a legal perspective.

However, the TelCo is required to retain location information and location identifiers that state an address from which a communication was received using an Internet access service provided by the TelCo; and was obtained by the TelCo as a result of providing OTT content and communications services. The destination IP addresses, the URL, port numbers and other Internet identifiers generated in respect of an OTT content and communications service are required to be retained (Explanatory Memorandum, 2015: p. 43) and disclose same ("*TIA Act 1979 (Cth)*," Sections 172 - 184).

The second exception

The Category A, B or C TelCo is not required to retain, and may therefore not be required to disclose, location information and location identifiers that relates to a communication that is being carried by means of another service and that is operated by a third party. This third party is using the relevant service operated by the Category A, B or C TelCo. The information could be contained in a physical document ("*TIA Act 1979 (Cth)*," Section 187A(4)(c)). The TelCo may be required to retain and disclose the information if it has it available (Explanatory Memorandum, 2015: pp. 43-44) and ("*TIA Act 1979 (Cth)*," Sections 172 - 184).

The general rule is, information and identifiers such as destination IP addresses, the URL port numbers and other Internet identifiers in respect of OTT content and communications services are required to be retained (Explanatory Memorandum, 2015: p. 43). However, if the latter data is generated from an OTT content and communications service that is operated by a third party that is using the telecommunications network of the TelCo to distribute the OTT content and communications service, the Category A, B or C TelCo is not required to retain the data ("*TIA Act 1979 (Cth)*," sections 172 - 184).

Both the Category A, B and C TelCo may provide managed services. A managed VoIP service, for example, is one purchased via the TelCo. The TelCo will typically provide the hardware such as the device and issue the phone number (ACMA, 2015: p. 41).

http://doi.org/10.18080/ajtde.v4n4.68

Generally speaking, in respect of e-mail and VoIP OTT content and communications services, the Category A, B and C TelCo is required to keep records of the destination IP address identifiers and port number (Explanatory Memorandum, 2015: p. 43): 'However, if a provider offers an additional OTT service, such as VoIP, it will be required to retain the relevant destination communication information' (A-G's Department, 2015: p. 22). The TelCo that is the provider of the VoIP service must retain the destination information for VoIP calls (A-G's Department, 2015: p. 22).

If the service is Skype or the like, that the Category A, B or C TelCo may not have control nor have visibility of the information. The service is just operating on the data stream, then its not the responsibility of the Category A, B or C TelCo to collect information about the device (Stanton, 2016) either. If the Category A, B or C TelCo does not provide the service, but it simply passes over the top of its telecommunications infrastructure, the Category A, B or C TelCo is not required to retain the location information or location identifiers in respect of that service or the device (Explanatory Memorandum, 2015: p. 44).

However, the position appears to be that the TelCo is granted the discretion to retain the location information and location identifiers, if the information is available to the Category A, B or C TelCo, whether it is a third party OTT content and communications service or an OTT content and communications service that is proprietary to the Category A, B or C TelCo: 'This item seeks to ensure that service providers are only required to retain telecommunications data to the extent that such information is available to that service provider' (Explanatory Memorandum, 2015: pp. 43-44).

The Category A TelCo that is the wholesaler to the MVNO (the Category B or C TelCo), is not required to retain the location information and location identifiers from the OTT content and communications services provided by the MVNO. The Category A TelCo, as the wholesaler is not required to inspect the IP packets of its reseller (the Category B or C TelCo) in an effort to "create" location information to ensure compliance with the law (A-G' s Department, 2015: p. 18). The parties may however commercially agree to retain location information and location identifiers on each other's behalf, because the information and identifiers must either be kept or cause to be kept ("*TIA Act 1979 (Cth)*," Section187A(1)).

The third exception

Location information and location identifiers about a telecommunications device, the TelCo does not use to provide the service the device is connected to, is not required to be retained ("*TIA Act 1979 (Cth)*," Section 187A(4)(e)). The Category C TelCo uses the location information and location identifiers for billing, as discussed above and must therefore retain same.

http://doi.org/10.18080/ajtde.v4n4.68

The Category A and B TelCo may not be required to retain location information and location identifiers in respect of OTT content and communications services provided by a third party that the Category A or B TelCo does not use itself. Location information and location identifiers to be retained are limited to information and identifiers that are used by the Category A, B or C TelCo in respect of the relevant service. Examples include information related to cell site location, Wi-Fi hotspots, or the Base Transceiver Station (BTS) the telecommunications device was connected to, at the start and at the end of the communication ("*TIA Act 1979 (Cth)*," Section187AA(1) item 6). The location information and location identifiers that are generated as the mobile device moves from tower to tower or from wireless access portal to portal, are not required to be retained whilst connected to the OTT content and communications service provided by a third party, that is simply using the network of the Category A or B TelCo (Explanatory Memorandum, 2015: p. 50).

The Category C TelCo is not obliged to create and retain detailed location records different to the location records used to provide the relevant service (Explanatory Memorandum, 2015: p. 44). The Category C TelCo is however not prohibited from doing so, as the statement from Telstra above indicates that it may use the available location information from a different service to disclose the latest location of the device (Burgess, 2015: p. 18). There are no specific retention and disclosure guidelines in the event any Category TelCo opts to do so. There are also no specific access and use guidelines in the event the law enforcement agencies opt to access detailed location records any Category TelCo may be in possession of.

The exceptions vis-à-vis the categories of entities

Irrespective of whether the Category A or B TelCo uses the location information and location identifiers, as long as the OTT content and communications services is provided over the network of the TelCo for which the TelCo is licensed to licence its retail customers in turn, the Category A or B TelCo is not required to retain the location information. The question however is whether the Category A or B TelCo is required to retain the location information, which includes location identifiers, if it does use the location information to provide the third party OTT content and communications services to which the device is connected. As described above, the telecommunications infrastructure does use the LCS functionality and retrieves the location information and location identifiers from the device or the network and delivers it to the application that requires it. The infrastructure does therefore use the location information to provide the service. The law is not clear on how it defines “used” in this context. Is it “used” when the TelCo issues the location identifiers to identify the device and to issue an invoice to the customer, or is it the fact that the network uses the identifiers to send the location estimates from the LCS server to the device across the network, or both, as described in Figure 1?

http://doi.org/10.18080/ajtde.v4n4.68

With regard to OTT content and communications services, which are instant messaging and social networking services, such as WhatsApp, Facebook and Twitter accessed via the public Internet by the individual customer over the IP network of the Category A, B, C TelCo, these TelCos are not compelled by law to retain and disclose any location information and location identifiers in this respect, as per the exceptions above, unless the TelCo has the information available. The Free and Invoiced Content and Communications Service Provider that does not have a carrier licence issued by the ACMA, and is not an ISP or a CSP, is not required by law to retain location information and location identifiers in respect of OTT content and communications services. The Free and Invoiced Content and Communications Service Providers are also not required to disclose the information to the Agencies ("*TIA Act 1979 (Cth)*," Section 187A(3)(b)(i) and (ii)).

The Free Content and Communications Service Provider would therefore also not be required to assist the agencies by disclosing location information it happens to possess. The Free Content and Communications Service Provider must be an ACMA-licensed TelCo to be compelled to provide assistance to the agencies ("*Telecommunications Act 1997 (Cth)*," Section 313(7)(d) and (e)). However, Free Content and Communications Service Providers and law enforcement agencies in most jurisdictions may enjoy good voluntary cooperation of sharing information sought by the agencies (Participant, 2016).

The Service Provider-Retention-Disclosure Obligation Relationship Table

Table 1 demonstrates the relationship between the type of service, the control of the network, the third party OTT content and communications service providers and the obligation of the TelCo to retain and disclose location information and location identifiers.

http://doi.org/10.18080/ajtde.v4n4.68

Table 1: The Service Provider-Retention-Disclosure Obligation Relationship Table

	Relevant Legislation
Control of Infrastructure	[Section 187A(3)(b) and (c) of the *TIA Act 1979 (Cth)]*
Service Provided	[Section 187A(4)(c) of the *TIA Act 1979 (TIA Act 1979)]*
Uses or does not use the location information	[Section 187A(4)(e) of the *TIA Act 1979 (Cth)]*
Retention Obligation	[Sections 187A(1), 187AA(1) and 187A(4)(b), (c) and (e) of the *TIA Act 1979 (Cth)]*
Disclosure Obligation	[Sections 276, 278, 280, 313(3) and (7) of the *Telecommunications Act 1997 (Cth)* and sections *172-183 of the TIA Act 1979 (Cth)]*
Power of agencies to access and use the information	[Sections 276, 278, 280, 313(3) and (7) of the *Telecommunications Act 1997 (Cth)* and sections 172-184 of the *TIA Act 1979 (Cth)]*

Service Provider	**The Category A TelCo**
Control of Infrastructure	Owns and controls the telecommunications infrastructure (access and core network).
Service Provided	Third-party licensed OTT content and communications service, e.g. Blackberry application.
Uses or does not use the location information	The network and the device uses the LCS functionality (location information and location identifiers) to provide the service the device is connected to. The TelCo may use some location identifiers to invoice the customer.
Retention Obligation	The TelCo is not obliged to retain location information nor the location identifiers. The TelCo may choose to retain location information and the location identifiers.
Disclosure Obligation	The TelCo is required to disclose the location information and location identifiers if it has the information available, under an authorisation issued by the agencies. The only URI the TelCo is not required to retain nor disclose without a warrant to the agencies, which appears to be considered content, is the URL.
Power of agencies to access and use the information	The law enforcement and national security agencies may authorise the TelCo to disclose the location information and location identifiers if the TelCo has the information available. The only URI the TelCo is not required to retain nor disclose without a warrant to the agencies, which appears to be considered content, is the URL.

http://doi.org/10.18080/ajtde.v4n4.68

Service Provider	**The Category B TelCo**
Control of Infrastructure	Leases the telecommunications infrastructure (access and/or core network) from the Category A TelCo.
Service Provided	Third-party licensed OTT content and communications services, e.g. Blackberry application.
Uses or does not use the location information	The network and the device uses the LCS functionality (location information and location identifiers) to provide the service the device is connected to. The TelCo may use some location identifiers to invoice the customer.
Retention Obligation	The TelCo is not obliged to retain location information nor the location identifiers. The TelCo may choose to retain location information and the location identifiers.
Disclosure Obligation	The TelCo is required to disclose the location information and location identifiers if it has the information available, under an authorisation issued by the agencies. The only URI the TelCo is not required to retain nor disclose without a warrant to the agencies, which appears to be considered content, is the URL.
Power of agencies to access and use the information	The law enforcement and national security agencies may authorise the TelCo to disclose the location information and location identifiers if the TelCo has the information available. The only URI the TelCo is not required to retain nor disclose without a warrant to the agencies, which appears to be considered content, is the URL.

http://doi.org/10.18080/ajtde.v4n4.68

Service Provider	**The Category C TelCo**
Control of Infrastructure	Owns or leases the telecommunications infrastructure (access and/or core network).
Service Provided	No third party operating the OTT content and communications service.
Uses or does not use the location information	The network and the device uses the LCS functionality (location information and location identifiers) to provide the service the device is connected to. The TelCo may use some location identifiers to invoice the customer.
Retention Obligation	The TelCo is obliged to retain the location information and location identifiers, because it uses the information to provide the service the device is connected to and/or there is no third party operator involved.
Disclosure Obligation	The TelCo is required to disclose the retained location information and retained location identifiers, if an authorisation is issued by the agencies. The only URI the TelCo is not required to retain nor disclose without a warrant to the agencies, which appears to be considered content, is the URL.
Power of agencies to access and use the information	The law enforcement and national security agencies may authorise the TelCo to disclose the location information and location identifiers

http://doi.org/10.18080/ajtde.v4n4.68

Service Provider	**The Category A, B and C TelCo**
Control of Infrastructure	Owns or leases the telecommunications infrastructure (access and/or core network).
Service Provided	Access to the public Internet
Uses or does not use the location information	The network and the device uses the LCS functionality (location information and location identifiers) to provide the service the device is connected to. The TelCo may use some location identifiers to invoice the customer.
Retention Obligation	The TelCo is not obliged to retain the location information and location identifiers in respect of an address to which a communication was sent on the Internet, from a telecommunications device and was obtained by the TelCo only as a result of providing access to the public Internet - The only URI the TelCo is not required to retain, which appears to be considered content, is the URL. However, the TelCo is required to retain location information and location identifiers that states an address from which a communication
Disclosure Obligation	The only URI the TelCo is not required to disclose without a warrant to the agencies, which appears to be considered content, is the URL. TelCo is required to retain location information and location identifiers that states an address from which a communication was received from on the Internet, from a telecommunications device, using an Internet access service provided by the TelCo and was obtained by the TelCo as a result of providing OTT content and communications services, if an authorisation is issued by the agencies.
Power of agencies to access and use the information	The law enforcement and national security agencies may authorise the TelCo to disclose the URL with a warrant. TelCo is required to disclose location information and location identifiers that states an address from which a communication was received from on the Internet, from a telecommunications device, using an Internet access service provided by the TelCo and was obtained by the TelCo as a result of providing OTT content and communications services, if an authorisation is issued by the agencies.

http://doi.org/10.18080/ajtde.v4n4.68

Service Provider	Invoiced Content and Communications Service Provider
Control of Infrastructure	The service is invoiced and used via the public Internet. The Internet is accessed via the network of the Category A and B TelCo
Service Provided	Licensed OTT content and communications services.
Uses or does not use the location information	The network and the device uses the location information to provide the service the device is connected to. The TelCo may use the location information and location identifiers to invoice the customer.
Retention Obligation	The provider is not obliged to retain the location information and the location identifiers
Disclosure Obligation	The provider is not obliged to disclose location information and location identifiers.
Power of agencies to access and use the information	The law enforcement and national security agencies request assistance from the provider to disclose information related to the device. The AFP announced that it will access and use geo-location information from social networking websites.

Service Provider	Free Content and Communications Service Provider
Control of Infrastructure	The service is provided and used for free via the public Internet. The Internet is accessed via the network of the Category A and B TelCo.
Service Provided	Free online OTT content and communications services, e.g. Twitter, Facebook, Instagram, Gmail and YouTube etc.
Uses or does not use the location information	The network and the device uses the location information to provide the service the device is connected to but the TelCo does not use the location information and location identifiers to invoice the customer because the service is free to the user
Retention Obligation	The provider is not obliged to retain the location information and the location identifiers
Disclosure Obligation	The provider is not obliged to disclose location information and location identifiers.
Power of agencies to access and use the information	The law enforcement and national security agencies request assistance from the provider to disclose information related to the device. The AFP announced that it will access and use geo-location information from social networking websites.

What the law gives, policy takes away

The limitations discussed above create a gap, whether deliberate or otherwise, in respect of the location information and location identifiers that could potentially be retained and

http://doi.org/10.18080/ajtde.v4n4.68

disclosed. This gap serves as an accidental privacy protection mechanism, although it may not have been deliberate, but it may be complemented with an undefined regime that exists in parallel to the Regime. This parallel regime creates the opportunity for the agencies to harvest location information from online social networks and using Big Data analytics to extract location information that could be used for law enforcement activities (Minister for Justice, 2016) and (Participant, 2016).

Funding was announced for the Australian Federal Police (AFP) for Big Data analysis of the data collected from social networking sites, as per the precedent set by the US Federal Bureau of Investigation (FBI) (Minister for Justice, 2016):

> Big data used in a law enforcement context provides a substantial mechanism to revealing threats and unlocking criminal plans hidden within *data-rich environments such as social media* or news reporting.
>
> The Coalition Government is funding this technology so our law enforcement agencies can engage the latest tools to overlay big data information with existing intelligence. ' (Minister for Justice, 2016: p. 1) (emphasis added).
>
> And
>
> *Open source social media provides a large data set* – subsequently providing linkages and other in depth intelligence on terrorist groups from their members (Minister for Justice, 2016: p. 1) (emphasis added).
>
> And:
>
> The sheer volume of associated data from the IS online onslaught has created a windfall of intelligence, and gives tremendous insight into terrorist organisations and also insight into operational activity from *geo-location*, to unintentionally leaked plans or photos, (Minister for Justice, 2016: p. 1) (emphasis added).

The reference to social media and insight into the geo-location of targets is a reference to the LCS functionality used in social network applications that are provided OTT. The legal exceptions discussed above places limitations on the TelCo to retain location information and location identifiers in respect of OTT content and communications services. The location information may not be sourced directly from the Category A or B TelCo, as social networking applications are OTT content and communications services provided by a third party, and therefore would be excluded from the retention obligations. The TelCo may therefore be unable to disclose the information the agencies seek. The law enforcement agency announced its intention to access location information directly from social media

http://doi.org/10.18080/ajtde.v4n4.68

posts instead. The law enforcement agency is accessing the information directly from the social networking content uploaded by the individual or by directly approaching the social networking website for assistance (Minister for Justice, 2016) and (Participant, 2016). The location information obtained from social networking websites may be used to complement the location information and location identifiers collected from the TelCo or to fill the gap. The question is whether this action requires a standardised governance framework, as is the case in respect of the TelCo.

The justification is that the information is OSINT. The individual may choose to disclose his/her location online. However, it is concerning that the law sends the message about data minimisation, by not requiring the retention of location information in respect of third party online applications on the one hand, but then does not address the harvesting of location information directly from the websites that is an OTT content and communications service. The user intends to only disclose its location to friends and family and may not accept to be trolled, even by law enforcement agencies without a judicial warrant.

The ASIO on the other hand, is adamant it is not trawling through data for security purposes. The ASIO stated to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) during the *Data Retention Bill 2014 (Cth)* hearings:

> We can only ever legislatively look for material, seek data, when we believe there is a nexus to security. We do not have the resources, ability, time, energy or inclination to be trawling. These are selective. We are looking at individuals of security concern. The concern expressed by some in the public — that we monitor communications of all Australians and that we are seeking to do that and that this would provide that — is erroneous. (Hartland, 2014).

Furthermore, the AFP requested the disclosure of MAC addresses directly from Apple (AFP, 2016: p. 18). This is because the TelCo may not have visibility of the MAC address (Participant, 2016). Apple is not a licensed carrier or a CSP and is therefore not subject to the Regime. Apple may be a Free Content and Communications Service Provider or an Invoiced Content and Communications Service Provider. Despite this, the law enforcement agency is requesting location identifiers from Apple.

It appears there may not be procedures in respect of obtaining assistance outside the realm of the Regime as set out in the *TIA 1979 (Cth)* and the *Telecommunications Act 1997 (Cth)*. It is not clear if the location information and location identifiers obtained are also restricted to the start and end of the communication, or whether the location information may even be sought during idle mode. This restriction is put in place to minimise the location information

http://doi.org/10.18080/ajtde.v4n4.68

accessed and used, and to prevent real world and cyber world tracking, as is the case in respect of the ACMA licensed TelCo.

The Big Data analytics announcement comes at a time when the uptake of OTT communications services has been skyrocketing the past four years:

> At May 2015, 65 per cent of adults had used social networking communications services and 42 per cent of adult Australians had used instant messaging in the previous six months, an increase of four percentage points on the same period last year (ACMA, 2015: p. 50).

Conclusions and Recommendations

Whereas the locally-licensed and locally-based TelCo is subject to retention and disclosure obligations, the Free and Invoiced Content and Communications Service Providers are not regulated. This situation is a cause for alarm to the industry:

> This is a real tension in our telecommunications regime, because, the metadata retention obligation is only applied to carriers and carriage service providers. You have to be 'a service for carrying communications or enabling communications carried by means of guided or unguided electromagnetic energy or both'. So, if you are an OTT provider, no metadata, unless you happen to be a service sold by a carrier or a CSP (Fair, 2016).

However it does not appear as if they are practically exempt. The agencies still request and obtain assistance from Free and Invoiced Content and Communications Service Providers and device manufacturers such as Apple. The social networking sites cooperate with law enforcement agencies and disclose information requested, even without the legal obligation to do so.

Whereas the law does not impose retention obligations in respect of third party OTT content and communications services on the TelCo, there is still a mandatory warrantless disclosure obligation attached in respect of the same location information and location identifiers, in the event the TelCo happens to possess the information.

The collection and analyses of location information from social networking websites undermines the legal exemptions that provide privacy protection, personal information protection and data minimisation.

The TelCo is not prohibited from retaining location information and location identifiers in respect of third OTT content and communications services. The duties set out the minimum limits and by doing so grants the TelCo the discretion to act beyond the minimum

http://doi.org/10.18080/ajtde.v4n4.68

requirements. No additional safeguards are provided for in respect of access to location information and location identifiers that is not required to be stored in the first place, such as a requirement to only disclose it with a judicial warrant. The lack of such a safeguards and the assistance by Free and Invoiced OTT Content and Communications Service Providers, undermine general privacy safeguards and is the OSINT lacuna in the law that may require addressing.

What the law gives with one hand, the operational activities of the law enforcement agencies take away with the other. It would appear that all the so-called privacy protections are seen simply as gaps to be filled by means of accessing location information from social networking websites, the regulation of which is not publicly known. What remains to be announced are the governance measures regarding the ethical access and use of location information from online social networking websites, and the internal and external *ex post and ex ante* oversight mechanisms.

The manner an individual chooses to access and use OTT content and communications services, or the manner the TelCo chooses to develop, acquire or distribute the service clearly dictates the power of access granted to the law enforcement agencies. It creates the power the agencies possess to access and use location information and location identifiers. It also dictates the level of privacy and personal information protection. The forum the individual uses to access and use a service, or the platform via which the service is provided, or the category of TelCo that provides the service, should not solely dictate privacy protections. In doing so, the Regime does not properly consider the full range of services, the infrastructure platforms used, the role players and the impact of reducing protections and increasing the powers of the agencies, in a contradictory manner.

The various formats of accessing and using communications need to be fully considered and the appropriate levels of protections, disclosure guidelines, discretionary retention by the TelCo and the open access by the agencies to information that would otherwise be restricted by law may need to be fully aligned to the Regime.

Acknowledgements

Thanks to Mr. John Stanton, CEO of the Communications Alliance; Mr. Patrick Fair, in his personal capacity, a telecommunications legal expert; and the Technical Expert Participant for providing great insight during the research interviews.

Thanks to UNSW, SEIT (ACCS, UNSW Law, D2D CRC) and to my individual Ph.D. supervisors.

References

Abbas, R; Michael, K; Michael, M. G; Nicholls, R. 2013. Sketching and validating the location-based services (LBS) regulatory framework in Australia. *Computer Law & Security Review, 29*, 576, 585, 587.

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

ACMA. 2016. 26 September 2016. Carriers & carriage service providers. Retrieved from <http://www.acma.gov.au/Industry/Telco/Carriers-and-service-providers/Licensing/carriers-carriage-providers-licensing-i-acma>

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

AMTA. 2010. AMTA guidelines location service providers for the use of mobile technology to provide passive location ‐ based services in australia. In AMTA (Ed.), (pp. 5, 9,). Sydney: AMTA.

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

Bell, P; Congram, M. 2014. Communication Interception Technology (CIT) and Its Use in the Fight against Transnational Organised Crime (TOC) in Australia: A Review of the Literature. *International Journal of Social Science Research, 2*(1), 46-66.

Cisco, S. I. 2016. Location Services. In I. Cisco Systems (Ed.), *MME Administration Guide, StarOS Release 21* (Vol. 21, pp. 297-310). California, USA: Cisco Systems, Inc. .

Clarke, R; Wigan, M. 2011. You are where you've been: the privacy implications of location and tracking technologies. *Journal of Location Based Services, 5*(3-4), 138–155. doi:10.1080/17489725.2011.637969

Cuijpers, C; Pekárek, M. 2011. The regulation of location-based services: challenges to the European Union data protection regime. *Journal of Location Based Services, 5*(3-4), 223-241. doi:10.1080/17489725.2011.637081

ETSI. 2016a. Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (pp. 22, 24, 25). Sophia Antipolis Cedex - FRANCE: ETSI.

ETSI. 2016b. Digital cellular telecommunications system (Phase 2+) (GSM);Universal Mobile Telecommunications System (UMTS);LTE; Functional stage 2 description of Location Services (LCS) (3GPP TS 23.271 version 13.0.0 Release 13) (pp. 12, 13,14,15,16,17,20,21,22,25,27,29,33,37,45,137,138-143, 145-154,). Sophia Antipolis Cedex - FRANCE: ETSI.

Hartland, K. 2014. *Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 17 December 2014, 19 (Kerri Hartland, Acting Director-General* House of Representatives.

Burgess, M. 2015. *Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 29 January 2015, 18 (Michael Paul Burgess, Chief Information Security Officer*.

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

European Parliament. 2015. *Over-the-Top (OTTs) players: Market dynamics and policy challenges*. (IP/A/IMCO/FWC/2013-046/). Belgium: EU Parliament Retrieved from <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/569979/IPOL_STU(2015)569979_EN.pdf>.

Fair, P. 2016. Interview with Patrick Fair (Sydney, M., 31 May 2016).

Gibson, S. 2004. Open source intelligence. *The RUSI Journal, 149*(1), 16-22. doi:10.1080/03071840408522977

Li, G. 2015. Regulating over-the-top services in Australia – from universal service obligation scheme to OTT regulation *International Journal of Private Law, 8*(1), 30-39.

Michael, G. E. K; Michael, M. G. 2011. The social and behavioural implications of location-based services. *Journal of Location Based Services, 5*(3-4), 121-137. doi: 10.1080/17489725.2011.642820

Minister for Justice. 2016. Minister for Justice and Minister Assisting the Prime Minister. 'Investing in innovation for our law enforcement elite' (Media Release, 15 June 2016).

Nicholls, R; Rowland, M. 2008a. *Lost in transcription: the Australian regime for interception of, and access to, communications content and metadata.* Paper presented at the Communications Policy and Research Forum 2008, Sydney. https://www.researchgate.net/publication/237011543_Lost_in_transcription_the_Australian_regime_for_interception_of_and_access_to_communications_content_and_metadata

Nicholls, R; Rowland, M. 2008b. Regulating the use of telecommunications location data by Australian law enforcement agencies. *Criminal Law Journal, 32*(6), 343-350.

Participant, I. w. A. E. 2016, 3 June 2016) *Research Interview/Interviewer: S. Shanapinda*.

Rodrick, S. 2009. Accessing telecommunications data for national security and law enforcement purposes. *Federal Law Review, 37*, 391.

Stanton, J. 2016. Interview with John Stanton, C. E. O., 8 July 2016.

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

Telecommunications (Interception and Access) Amendment (Data Retention) Act (No 39) 2015 (Cth).

Telecommunications Act (No 47) 1997 (Cth).

Telstra. 2014. Part H – BigPond Mobile Services (previously known as Telstra Active or WAP), 5,39-42, . Retrieved from www.telstra.com.au website: <https://www.telstra.com.au/content/dam/tcom/personal/consumer-advice/pdf/consumer/infoservices.pdf>