GILBERT +TOBIN

MANDATORY INTERNET DATA RETENTION IN AUSTRALIA

EVIDENTIARY USES AND CHALLENGES

WRITTEN BY PETER LEONARD - Director, iappANZ

MARCH 2016

diGiTal

CONTENTS

INTRODUCTION

The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (in this article, the '2015 Act') made important and controversial amendments to the Telecommunications (Interception and Access) Act 1979 ('TIA Act') and the Telecommunications Act 1997.

Proposals for mandatory data retention for communications services has engendered criticism and controversy in many countries. Pervasive and extensive communications data collection and retention has been stated by many Governments, including the Australian Government, as necessary to address new threats of internet facilitated terrorism, child exploitation and human trafficking. Criticisms as to pervasiveness have been met with government reassurances as to limitations as to who can access and some safeguards as to permitted access and use.

Reflecting these reassurances, the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (2015 Act) passed through the Australian Parliament with a remarkable degree of bi-partisan support. Amendments to the Bill included a few safeguards suggested by critics of the Bill, but the scope of mandatory data retention remained largely unchanged from the Government's initial proposals.

As compared to other advanced industrialised democracies, telecommunications service providers in Australia are now subject to the most stringent requirements to collect and retain data about use of telecommunications services by users.

Australia also has a relatively low level of independent scrutiny and oversight of exercises by law enforcement agencies of their powers to access that data.

A number of the safeguards on access to and use of mandatorily retained data are of particular interest to litigators and privacy professionals. This article principally concerns one safeguard which has been the subject of surprisingly little comment. That safeguard is certain conditions imposed upon release of mandatorily retained communications data to persons other than intelligence services and law enforcement agencies empowered by provisions of the 2015 Act to access that data, particularly in the context of civil litigation. The 2015 Act revised pre-existing safeguards on disclosure, initially (and potentially only as an interim measure) limiting the circumstances in which the mandatorily retained data of telecommunications providers can be disclosed. The scope of data sets to be mandatorily retained by telecommunications service providers, and rights of access to that data by intelligence services, law enforcement agencies and potentially other persons, are the central points of focus of this paper.

AUSTRALIAN TELECOMMUNICATIONS INTERCEPTION AND ACCESS LAW

Australian telecommunications law is rightly seen as an arcane and obscure field of law. At the depths of obscurity lie the laws addressing access to information about communications or (as now notoriously incorrectly described) 'telecommunications metadata'.[1]

The reason for that obscurity issue can be simply stated. The law of telecommunications interception was developed to protect the expectations of confidentiality of two humans speaking to each other over a copper wire operated by the Post Master General. In a world now long gone, where 'privacy' had not entered the Australian legal lexicon and Mark Zuckerberg had neither been born nor declared privacy dead, two humans when speaking to each other had a reasonable expectation that their spoken communication would not be monitored or reported to others (except when they chose to argue on a stage or soapbox or in a crowded public place). Similarly, humans when communicating to each other within envelopes using a quaint custom now described as snail mail, had a reasonable expectation that their sealed envelope would not opened, examined or otherwise used by the State.[2] Telephonic communications were protected long before general privacy laws: it was an offence to tap or record the content of spoken communications transmitted down those copper wires without the knowledge and informed consent of the humans speaking those words, except in those very unusual circumstances where the sanctity of a private communication was overridden by public interest. Judicial oversight of third party wire taping or recording was considered appropriate and hence a judicial warrant was required.[3]

By contrast, information about communications – in fixed telephone call days, the dialling number, the number dialled and the duration of the call – was rightly regarded as less sensitive, albeit still confidential. Given the lower level of sensitivity of information about communications as compared to the content of communications, the procedures to permit lawful access to information about communications were 'light touch' when compared to the warrants regime for interception of call content.

By section 177 of the TIA Act and predecessor provisions[4], a telecommunications carriage service provider could voluntarily disclose information about communications to an enforcement agency if the disclosure was reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty or for the protection of public revenue.

Pursuant to section 178 and section 179 of the TIA Act, an authorised officer of an enforcement agency may give a written notice to a telecommunications carriage service provider (CSP) which had the effect of authorising access to existing documents or existing information about communications by an authorised officer of that agency, where purportedly reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty, or for the protection of public revenue.

Enforcement agencies so authorised included a body whose functions included administering a law imposing a pecuniary penalty or administering a law relating to the protection of public revenue.[5] In 2012-13 data was accessed by around 80 Commonwealth, State and Territory agencies with law enforcement or revenue protection functions.[6] And so local councils, pasture protection boards and diverse other bodies joined more well-known enforcement agencies such as the Australian Federal Police and State Police and Crime and Corruption Commissions in enjoying written authorisation powers – effectively, of self-certification – that enabled that agency to obtain access to information about communications, but not access to content of communications. The power of self-certification was however somewhat constrained: the authorised officer of the agency was required to not make the authorisation unless he or she was satisfied that the disclosure was reasonably necessary for the enforcement of the criminal law.[7] Nonetheless, the number of requests for access steadily grew: between July 2013 and June 2014 over 550,000 requests for information

1. A useful review of telecommunication data retention proposals before the 2015 Act is provided in Nigel Brew, Telecommunications data retention: an overview, Parliamentary Library, Canberra, 24 October 2012, available at http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BN/2012-2013/DataRetention.
2. Whether that expectation was in fact reasonable might now be questioned, at least in the U.S.A. : see Office of the Inspector General of the United States Postal Service Audit Report – HR-AR-14-001, 28 May 2014 available at https://www.uspsoig.gov/story/audit-report/protecting-mail-covers-law-enforcement-investigations#.VUbbyk0cQei and as reported by Ron Nixon, 'Lawyers' Group Seeks Overhaul of a Postal Service Surveillance Program', New York Times, 21 April 2015, as available at http://www.nytimes.com/2015/04/22/us/report-seeks-overhaul-of-postal-service-surveillance-program.html?_r=0.
3. See for example section 4 of the Telephonic Communications (Interception) Act 1960 and section 7 of the Telecommunications (Interception) Act 1979 as respectively enacted, as available at http://www.comlaw.gov.au/.
4. For example, section 47(2) (AUSTEL, carriers and service providers to prevent use of networks and facilities in commission of offences) of the Telecommunications Act 1991.
5. Definition of 'enforcement agency' in section 5 of the TIA Act as enacted and as amended prior to the 2015 amendments.
6. Revised Explanatory Memorandum, para [10], page 3.
7. Section 178(3) of the TIA Act as enacted and as amended prior to the 2015 amendments.

about communications were made by Australian law enforcement agencies of Australian communications carriers and carriage service providers. This statistic does not appear to include requests made under lawful authority outside the Telecommunications (Interception and Access) Act 1979.

Many other Federal, State and territory laws can compel any person holding that information to provide that information, potentially including information about communications, to a wide range of bodies and individuals.

In addition, judicial officers of various courts and tribunals regularly issue subpoenas requiring production of documents, including carrier records about telecommunications users. There are no reliable records as to the number of such requests.

The TIA Act was amended in October 2012 to require preservation of certain stored communications stored on equipment operated by or in possession of an Australian carrier or carriage service provider, pursuant to:

+ a domestic preservation notice, issued by either a law enforcement agency (a broad range of State and federal agencies are listed in section 5 of the Act) or in the case of (live) interception, a more limited class of interception agencies; or
+ a foreign preservation notice, issued by the Australia Federal Police following a Mutual Legal Assistance Treaty (MLAT) request made by a foreign law enforcement agency.

The subject matter of these preservation notices was 'stored communications', which had been interpreted to mean what is commonly referred to variously as call content and the content of communications or payload data, but not information about communications (i.e. service identifiers, device identifiers such as MSISDN, location related information, date, time duration etc.). A domestic preservation notice could only be issued for a 30 day period. It could then be replaced by a telecommunications service warrant (either an interception warrant or a stored communication warrant) issued in respect of a particular person and valid for preservation of communications content of specified types of communications made by that particular person within a specified period.

The 2015 Act was a radical departure from the previous statute law by being the first mechanism to mandate a requirement to preserve of information about communications on a generic, service-wide basis, not case by case in response to a specific request. The aspect of the law which appeared to most concern law enforcement agencies was what they argued was a lacuna in the law: no law required a telecommunications carrier to collect and retain particular categories of information about communications.

As in many other areas of business, if the record was there it could be accessed under statutory process or by court-issued subpoena or notice to produce, but whether it was collected and retained was for the carrier to determine.

So what has changed that made telecommunications different from these other areas of business and justified a requirement for new data retention laws?

IMPORTANT TRENDS THAT LED TO NEW DATA RETENTION LAWS

What people do, where they do it and who they do it with, has become more easy to 'read' through observing the electronic data that surrounds them than by physical surveillance. This fundamental change has principally been the outcome of the increasing range of uses of communications and arrival of mobile phones, then social media, then smart phones and apps, and now and into the future other personal internet devices such as eHealth devices.

It is easy now to forget that phones were once primarily associated with a household, a workplace or a public place, rather than a particular individual. When the late Steve Jobs unveiled the iPhone in 2007, he promised: "This will change everything". Seven years later over two billion people around the globe own a smartphone. In Australia, mobile phone penetration is 140% and over 75 percent of Australians use a smartphone.

Non 'digital natives' once lamented that their teenage kids told the story of their lives in their electronic interactions. Now they have joined them. But the story is much richer than the content of those interactions: the 'real' story of most of our lives is now not in what we say, but what we do, as potentially disclosed through analysis of information about electronic communications. This 'digital exhaust' that surrounds and trails after the actual content of communications is no longer a waste product, but increasingly a valuable product in itself. Today all generations carry a smart phone logged into a network and various apps and services variously in use throughout most waking hours of the day. Many individuals are active in various kinds of social media: Facebook has over 14 million active Australian users, Twitter about 3 million and Tumblr about 4.25 million. The digital exhaust of those interactions chronicles each individual's solitary life and the individual's social interactions. A rich picture assembles of each person's solitary and social life if and when an observer is able to put together the time stamped, geo-located cellular, Wi-Fi and Bluetooth track of a mobile phone, the serial record of mobile broadband internet activity (including social media interactions) of an individual, the incidental output of devices such as vehicle toll tags, Fitbits and surveillance cameras in public places, and card based financial and retail transactions conducted by that individual.

It should therefore not be surprising that what an individual does, where that individual did it and who with, is often much more valuable to intelligence and law enforcement agencies than what that individual said. It is sometimes suggested that if a policy maker was today to undertake a clean slate development of laws governing access to communications, the existing regime would be inverted, with warrants required for access to most information about communications and a lower level of authorisation, such as self-certification by criminal law enforcement agencies, for interception of content of specific communications.

So what factors currently limit the extent to which each and all of us become the fictional character Winston Smith as pervasively observed by Big Brother in George Orwell's *1984*?

Firstly, there have been significant constraints that are both technological (including cost) and regulatory upon information about communications being collected at all, or retained and transformed into formats capable of analysis. 90% of the data in the world today has been created in the last two years alone.[8] Even with big data analytics, there is much more data than it makes sense to retain for any extended period or to seek to analyse either at all or other than for very limited purposes. Furthermore, even with the rapid decline in costs of storage and of analytics, data volume and diversity create complexity and therefore expense to collate and retain data, often overwhelming commercial utility. That said, partially funded (by Federal subsidy) mandatory data retention reduces that cost constraint.

The second constraint is that each individual's communications interactions are intermediated by a diverse range of telecommunications service providers, often providing services in several layers over each other. So my personal Telstra mobile phone and work mobile broadband account might be used for private Skype (Microsoft) mobile voice and video calls, tweets, communications through Google Hangouts, interactions with friends through Facebook and Facebook Messenger, Snapchats, deposits to and retrievals from Dropbox, and so on. Many service providers have no physical presence in Australia. Many service providers facilitate anonymise use and/or strong encryption of communications passing over their servers.

Australian law enforcement agencies therefore increasingly focus attention upon the providers of access to communications services and the underlying communications connectivity that enable other internet services to be provided 'over the top' (OTT) of those access and connectivity services, because these providers are both amenable to Australian jurisdiction and platforms over which many other services are provided. However, these providers may not collect information about the OTT services at all, or in any useable form, because that information is not required for the conduct of their own business. Hence Telstra, Optus, Vodafone, iiNet, TPG and other fixed and mobile broadband service providers operating in Australia became key players in Australian law enforcement but may not collect information about communications related to OTT services that enforcement agencies would like to be collected and retained by them unless mandated to do so.

The third constraining factor is closely related to the second. A key trend in fixed and mobile broadband service offerings over the last ten years has been a movement away from metered communications interactions to flat rate ('all you can eat') services. If use of services is not relevant to billing, information about particular uses of services becomes less important, and this less important information is therefore less likely to be kept than other, more commercially, useful data. This led to the Australian Government suggesting that mandatory data retention laws were necessary and justified because (the Government alleged) Australian fixed and mobile broadband service providers were collecting and retaining less information about communications than was previously the case. Such evidence as there may have been for this allegation appears to have been given in secret briefings to Government by intelligence organisations and criminal law enforcement agencies. No definitive evidence of this alleged trend appears to have been put on the public record. On its face this alleged trend appears counter-intuitive given the declining costs of storage of data and perceived growth in the value of data analytics conducted across big data sets. In any event, the Government stated that it had significant and growing concerns that the decline in capture of information about communications and that the valuable information about communications was increasingly in respect of use of OTT services higher up the communication 'stack', which the underlying providers of access and connectivity professed no interest in capturing and retaining. And hence a key aspect of the metadata retention debate has been discussion as to whether data retention should be mandated to require Australian-based underlying providers of access and connectivity to capture and retain information about use of OTT services passing over their access and connectivity services – and if so mandated, as to how much this would cost and what proportion of this cost should be borne by the Government.

The fourth factor is the operation of privacy law in relation to personal information as compared to collection of other information which does not enable an individual to be identified or reasonably identifiable. Many services that depend upon collections of commercially valuable information can be facilitated through use of non-personally identifying information even if the sign-up process entails collection of personal information (for example, to facilitate a credit card payment). Australian privacy law does not operate to constrain uses of reliably and verifiably de-identified information, which may nonetheless be re-identifiable when passed into the hands of law enforcement agencies through

8. http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html.

mandated data access. The scope of protection through Australian privacy law is increasingly difficult to determine for two reasons. The first is the rapid increase in diversity of data collection points around each individual, many of which do not involve human intermediation in specifically and knowingly authorising collection of data through the use of a particular device. The second is the diverse, inconsistent and often poorly documented quarantining processes of individual corporations in relation to their handling of personal information.

The increasing diversity of data collection points received scant attention in the Parliamentary debates about mandatory communications data retention. Consider the table below, as published by the OECD in January 2013. It describes a household of two adults and two teenagers living in an advanced post-industrial country like Australia in each of 2012, 2017 and 2022.[9] The projections as to number and range of devices are probably conservative: in particular, eHealth devices, enabling close monitoring as to an individual's physical activity, now appear likely to be ubiquitous well before 2022. In any event, it is clear that the rich picture described above as to most individuals' solitary lives will shortly be further enhanced by details of their movements and interactions within the home, usually reported by a device activated by a user without much thought as to possible secondary uses of data collected through the device or about the operation of the device. The activation of such purpose specific devices is often not recognised by most consumers as a privacy issue at all, perhaps because provision of personal information through the sign-up process is not associated in the consumer's mind with any secondary uses that might be made of information associated with the service. And who has the time to read all these privacy statements anyway?[10] By 2022 the bathroom and the bedroom may remain mute (this author hopes), but in most other areas of the home, the workplace, and places of activity in between, some device will be reporting some information to some application somewhere.

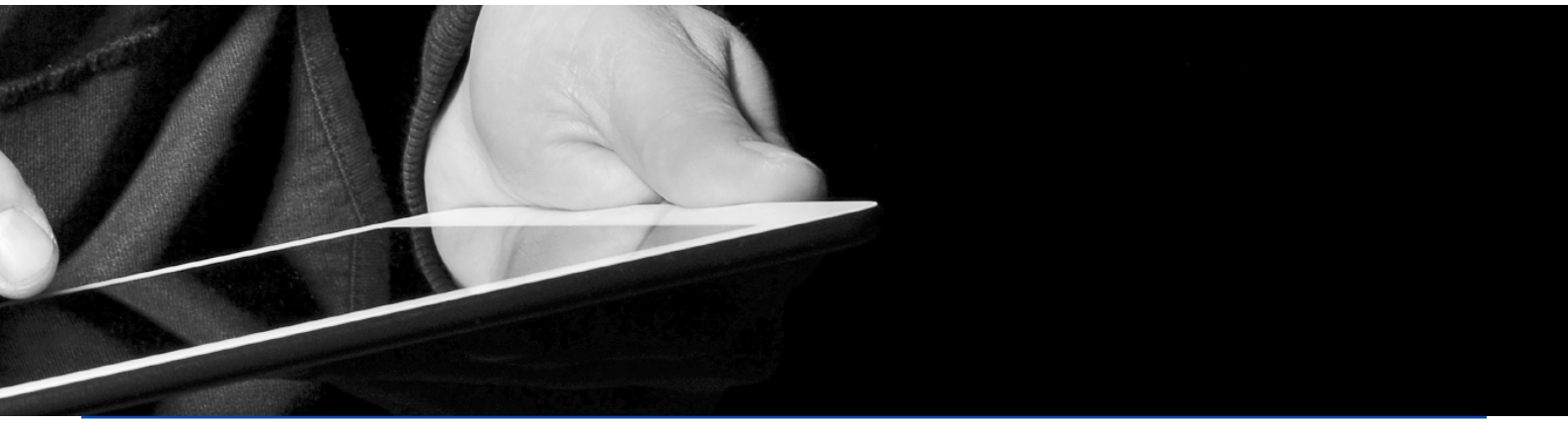
So should we be concerned? We now turn to consider what must be collected and by whom and then the restrictions upon access to that data.

9. OECD Building Blocks for Smart Networks, OECD Digital Economy Papers No. 215, January 2013, available at http://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826.

10. Estimates vary, but the most frequently cited study appears to be the study conducted in 2008 by researchers at Carnegie Mellon University, Aleecia M. McDonald and Lorrie Faith Cranor, which found that it would take the average reader about 250 working hours every year, or about 30 full working days, to actually read the privacy policies of the websites they visit in a year. This controlled study does not appear to have been updated since 2008 to account for apps, growth in diversity of online content sites and social media: it is likely therefore that the estimate is now far too conservative. See Aleecia M. McDonald and Lorrie

2012	2017	2022
2 smartphones	4 smartphones	4 smartphones
2 laptops/computers	2 laptops	2 laptops
1 tablet	2 tablets	2 tablets
1 DSL/Cable/Fibre/Wifi Modem	1 connected television	3 connected televisions
1 printer/scanner	2 connected set-top boxes	3 connected set-top boxes
1 game console	1 network attached storage	2 e-Readers
	2 e-Readers	1 printer/scanner
	1 printer/scanner	1 smart meter
	1 game console	3 connected stereo systems
	1 smart meter	1 digital camera
2012	2017	2022
	2 connected stereo systems	1 energy consumption display
	1 energy consumption display	2 connected cars
	1 Internet connection car	7 smart light bulbs
	1 pair of connected shoes	3 connected sports devices
	1 pay as you drive device	5 internet connected power sockets
	1 network storage	1 weight scale
		1 eHealth device
		2 Pay as you drive devices
		1 intelligent thermostat
		1 network attached storage
		4 home automation sensors
Devices that are likely but not in general use		
eReaders	Weight scale	Alarm system
Sportsgear	Smart light bulb	In house cameras
Network attached storage	eHealth monitor	Connected locks
Connected navigation device	Digital camera	
Set top box		
Smart meter		

Source: *OECD, Building Blocks for Smart Networks, OECD Digital* Economy Papers No. 2015, January 2013.



WHO IS REGULATED? PROVIDERS OF COMMUNICATIONS CARRIAGE SERVICES

Communications carriage services are services for the carriage of voice, audio, visual, audio-visual and any other form of data between distinct places.[11] Provision of such carriage services to the public[12] within Australia using certain types of communications capacity leads to the owner of that capacity being required to be licensed as an Australian telecommunications carrier.[13] Use of such capacity within Australia, or to and from Australia, to provide carriage services to the public leads to the provider of such carriage services being required to comply with requirements in the Telecommunications Act 1997 and the TIA Act that are applicable to 'carriage service providers' ('**CSP**').[14] An 'internet carriage service' is a particular category of carriage service that enables end users to access the internet and that service is provided by an internet access provider, sometimes also referred to as an internet service provider ('**ISP**'). So an internet access provider will usually be a CSP because the provider provides to its users carriage of traffic over the internet (as well as internet connectivity) and also an 'ISP.

However, although ISP is a term of art in Australia[15] it is used in many different contexts and may be any of a service provider that is required to also be a carrier, a CSP, or neither (i.e. Facebook and many content service providers). An ISP will be required to be licensed as a carrier if the ISP owns 'network unit' capacity in Australia that is used by it or others to provide carriage services within Australia or to and from Australia to the public: for example, iiNet is a carrier, as well as an ISP and CSP. A VoIP provider such as Skype carries voice traffic over the internet as well as out to non-Skype numbers and is a CSP. But a provider of cloud services on a 'meet me' or 'come-to-me' basis – Dropbox, Amazon Web Services, etc. – is not a CSP, unless the provider also branches out to deliver communications traffic to the public. Many service providers provide internet carriage services to and from Australia and to the Australia public 'over the top' (OTT) of other internet carriage services. This means that some OTT service providers are regulated (because of the carriage component of their service) as CSPs, regardless of whether they own or operate telecommunications network infrastructure in Australia. This frequently leads to knotty legal questions as to whether a service is a regulated carriage service. Even more confusingly, what is a very important regulatory distinction under the Telecommunications Act as between carriers and CSPs is glossed over in some parts of that Act and the TIA Act that deem carriage service providers to be carriers for the purpose of application of those Parts. For example, except in Parts 5-4 (which relates to the requirement for licensed telecommunications carriers to prepare and file interception capability plans) and 5-4A (which relates to the requirements for licensed telecommunications carriers to provide advance notification to the Communications Access Coordinator as to planned network changes) of the TIA Act, 'carrier' is defined[16] to also include 'carriage service provider', so references throughout most of the TIA Act to carriers must be read to also include CSPs.

The 2015 Act applies mandatory data collection and retention to:

+ services as set out in section 187A(3) of the amended TIA Act, being service for carrying communications, or that 'enable' (a new concept) communications to be carried, by guided or unguided electromagnetic energy or both;
+ services as 'operated by' (a new concept) a carrier or a ISP,
+ a service if the person operating the service that owns or operates 'infrastructure' in Australia that is used in the provision of any service as set out in section 187A(3) of the amended TIA Act (that is, not each and all of the services that it provides as set out in section 187A(3)).[17]

The complexity of the 2015 Act largely arises out of these intertwined concepts and related exceptions that affect the scope of services and information required to be kept about those services. Analysing this complexity is outside the scope of this paper: for current discussion, suffice it to summarise that subject to some exceptions and qualifications, and also potential extensions by Ministerial direction, carriers and ISPs:

+ are required to keep the kinds of information about services specified by new section 187AA of the TIA Act about the use of OTT services that is available to them in the course of, or as an incident of, their provision of the underlying service, but
+ are not required to institute active steps to collect and then keep additional information that might be capable of being captured in relation to the OTT service that otherwise would fall within the kinds of information about services specified to be collected and kept by new section 187AA of the TIA Act.

11. Definition of 'communications' and of 'carriage service' in section 7 of the Telecommunications Act 1997.
12. Section 42 of the Telecommunications Act 1997.
13. Section 42 of the Telecommunications Act 1997 and definitions of 'network unit' in Division 2 of Part 2 of the Telecommunications Act 1997.
14. Definition of 'carriage service provider' in section 87 of the Telecommunications Act 1997, of 'supply to the public' in section 88 and of 'listed carriage service' in section16 of that Act.
15. As defined in clause 8 of Schedule 5 to the Broadcasting Services Act 1992.
16. Definition of 'carrier' in section 5 of the TIA Act.
17. Section 187(3)(c) of the TIA Act as amended by the 2015 Act,; see also Revised Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Revised Explanatory Memorandum), at para [230].

WHAT INFORMATION MUST BE COLLECTED AND RETAINED?

Providers of relevant telecommunications services are required to retain telecommunications data associated with a communication specified in subsection 187AA for a period of two years.[18]

Section 187AA lists the "kinds of information" that service providers must collect and retain in relation to each relevant service that they provide. "The detailed, technologically-neutral table in subsection 187AA(1) is designed to ensure that the legislative framework gives service providers sufficient technical detail about their data retention obligations while remaining flexible enough to adapt to future changes in communication technology."[19]

If the information or documents that service providers are required to keep are not created by the operation of the relevant service or if only created in a transient form, then the service provider is required to use other means to create this information.[20]

The mandatory data set is summarised in the table[21] attached to this paper. The kinds of information that a service provider must keep include:[22]

- the users of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service, e.g. customer identifying details, such as name and address; customer contact details, such as phone number and email address; unique identifying number attached to a mobile phone or the IP address (or addresses) allocated to an internet access account or service; billing and payment information; roaming information; but not passwords, PINs, secret questions or token codes which are used for authentication purposes;
- source information: identifiers of a related account, service or device from which the communication is sent by means of the relevant service, e.g. the phone number, IMSI, IMEI from which a call or SMS was made; identifying details (such as username, address, number) of the account or service or device from or over which the communication was made; the IP address and port number allocated to the subscriber or device connected to the internet at the time of the communication;
- destination information: identifiers of the account, telecommunications device or relevant service to which the communication is sent, or where it is forwarded, routed or transferred, similar to source information but excluding "anything that is web-browsing history or could amount to web-browsing history, such as a URL or IP address to which a subscriber has browsed";
- the date, time and duration of a communication or of connection to a relevant service. This does not include intermediate points throughout a communications session, such as individual updates to multiple applications running in the background on a smartphone connected to a mobile data network (the near-continuous stream of communications together constituting a single communications session);[23]
- the type of communication (e.g. voice, SMS, email, chat, forum, social media); the type of the relevant service (e.g. ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE); and the features of the relevant service used or enabled for the communication (e.g. call waiting, call forwarding). The Revised Explanatory Memorandum also states in relation to this item that "Data volume usage, applicable to internet access services, refers to the amount of data uploaded and downloaded by the subscriber. This information can be measured for each session, or in a way applicable to the operation and billing of the service in question, such as per day or per month".[24] However, the Table in section 187AA does not refer to "data volume usage", leaving doubt as to whether this is within the kinds of information prescribed to be captured and retained;
- the location of the relevant access at the start of the communication and at the end of the communication (e.g. by cell towers or Wi-Fi hotspots). The Revised Explanatory Memorandum states: "Service providers are not required to keep continuous, real-time or precise location records, such as the continuous GPS location of a device. These limitations seek to ensure that the location records to be kept by service providers do not allow continuous monitoring or tracking of devices".[25]

The data retention requirements expressly do not require a service provider to collect and retain:

- the contents or substance of a communication, which includes an email subject line;[26]
- information that states an address (e.g. uniform resource locators (URLs), internet protocol (IP) addresses, port numbers and other internet identifiers with which a person has communicated via an internet access service provided by the service provider, where that information was obtained by

18. Section 187C.
19. Revised Explanatory Memorandum, para [225].
20. Section 187A(6).
21. As available for download at https://www.ag.gov.au/dataretention.
22. Reading together the Table in section 187AA(1) and the Revised Explanatory Memorandum, pages 46 to 50.
23. Section 187AA(5).
24. Revised Explanatory Memorandum, para [252], page 49.
25. Section 187A(4)(a), Revised Explanatory Memorandum, para [252], Item 6, page 50.
26. Revised Explanatory Memorandum, para [236], page 42.

the service provider only as a result of providing the service.[27] This exception is stated to exclude only web browsing history from the retention scheme. If the service provider obtains a destination internet address identifier in the course of providing another service, the provider would be required to keep records of such identifiers. The Revised Explanatory Memorandum states: "For example, an email service provider is required to keep records of the destination internet address identifiers associated with the use of an email service, such as the email and IP address, and port number to which an email was sent. Similarly, if a service provider that provides an internet access service to a subscriber also provides a Voice over the Internet Protocol (VoIP) service to that subscriber, the service provider is required to keep records of any destination internet address identifiers associated with the use of that VoIP service. This could include the internet protocol (IP) address to which a VoIP call was sent. In this example, however, the service provider is not required to keep records of any other destination internet address identifiers associated with web browsing"[28]; or

+ information to the extent that it relates to a communication that is being carried by means of another service that is of a kind referred to in paragraph 187A(3)(a) and that is operated by another person using the relevant service operated by the service provider. We have already discussed the difficulties in interpreting the relevant provisions in relation to OTT services.

DATA SECURITY

One of the criticisms of the data retention requirements is the potential that this scheme creates for data breaches and intrusions.

By way of response to such criticism, section 187BA provides that a service provider must protect the confidentiality of information that the service provider must keep by encrypting the information and protecting the information from unauthorised interference or unauthorised access. The section does not prescribe a particular type of encryption. Section 187LA of the amended TIA Act supplements the obligations of service providers under Australian Privacy Principle (**APP**) 11.1 to "take such steps as are reasonable in the circumstances to protect [personal] information from misuse, interference and loss; and from unauthorised access, modification or disclosure". Carriage service providers are already required pursuant to clause 4.6.3 of the Telecommunications Consumer Protection Code (C628:2015)[29] to have "robust procedures to keep its Customers' Personal Information in its possession secure and restrict access to personnel who are authorised by the Supplier". However, these obligations attach only to personal information as defined in and regulated by the *Privacy Act 1988*.

Section 187LA provides that the Privacy Act applies to all service providers to the extent that the service provider's activities relate to retained data, and that Information that is kept to fulfil the data retention requirements "is taken, for the purposes of the Privacy Act 1988, to be personal information about an individual if the information relates to an individual or a communication to which the individual is a party". This unusual provision appears to operate as a statutory deeming of information kept to fulfil the statutory obligation to collect and retain information about relevant services to be personal information, although apparently not also extending to other information that carriers may collect and retain for commercial purposes which is not by its nature personal information as defined in the *Privacy Act 1988*.[30]

It also follows that individuals will be able to request access to retained data relating to them (whether or not otherwise 'personal information' as defined in the Privacy Act) in accordance with APP 12. Consistent with the APPs, service providers will be able to charge an individual for providing access to this information. It should be noted that the right of individuals to request access to personal information held by any APP entity about them is seldom exercised but remarkably broad and potentially a valuable tool for prospective litigants. Although the scope of what is 'personal information' that is subject to an individual's right of access has recently put into question by the decision of the Australian Administrative Appeals Tribunal in Telstra Corporation Limited and Australian Privacy Commissioner [2015] AATA 991, 18 December 2015, now under appeal to the Full Federal Court of Australia, the broad operation of the right itself appears quite clear. In that case the Tribunal overturned the earlier determination by the Australian Privacy Commissioner granting journalist Ben Grubb access to certain data relating to Mr Grubb's use of Telstra mobile services. The Tribunal's Decision threw open the issue of how to work out when device information is 'about an individual whose identity may be reasonably ascertained from the information'.[31]

27. Section 187A(4)(a), Revised Explanatory Memorandum, paras [240] and [241], page 43.

28. Section 187A(4)(a), Revised Explanatory Memorandum, para [241], page 43.

29. As available at http://www.acma.gov.au/~/media/Networks/Regulation/pdf/C628_2015%20Telecommunications%20Consumer%20Protections%20Code%20pdf.pdf.

30. For recent discussion as to the characterisation of information held by a carrier and whether it is personal information that therefore is subject to the right under the Privacy Act for an individual to access personal information held about them, see Ben Grubb and Telstra Corporation Limited [2015] AICmr 35 (1 May 2015), available through http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-determinations/2015-aicmr-35.

31. The reasoning underlying the Tribunal's decision is critically reviewed in the author's forthcoming paper Peter Leonard A review of Telstra Corporation Limited and Australian Privacy Commissioner, E-Commerce Law Reports Volume 16 Issue 01 (March 2016).

WHICH AGENCIES OR OTHER PERSONS CAN ACCESS RETAINED INFORMATION?

The Federal Privacy Act 1988 exempts certain disclosures in 'permitted general situations', including that the disclosure "is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim".[32]

Disclosure is also permitted where the disclosure "is required or authorised by or under Australian law or a court/tribunal order".[33] There are many such laws: a variety of Federal, State and Territory Acts empower particular agencies to compel disclosure. For example, section 29 (Power to obtain documents and things) of the Crime Commission Act 2012 (NSW) provides that an executive officer of the NSW Crime Commission with special legal qualifications may, by notice in writing served on a person, require the person to attend before the Commission at a particular time and place and produce to that officer a document or thing specified in the notice, being a document or thing that is relevant to an investigation. In addition, subpoenas are frequently issued by courts on third parties, including carriers and CSPs, to produce records in a wide range of civil litigation.

Information about communications currently cannot be disclosed by carriers or CSPs because to do so would lead to criminal liability under (most relevantly) section 276 of the Telecommunications Act 1997 and possible contractual liability to the user and/or liability under privacy laws and associated telecommunications codes with privacy-related provisions, such as the Telecommunications Consumer Protections (TCP) Industry Code (C628:2012).

Exceptions to section 276 that were already in operation before the 2015 Act allowed carriers and carriage providers to elect to make voluntary disclosure if "the disclosure is reasonably necessary for the enforcement of the criminal law" or "a law imposing a pecuniary penalty or for the protection of the public revenue".[34] In practice most providers elected not to make voluntary disclosure of information about communications because of prospective liability that might flow from them making an inherently subjective determination as to what is, or is not, "reasonably necessary", and the fact that voluntary disclosures generally are not excepted from privacy laws and associated telecommunications codes with privacy-related provisions.

32. Section 16A of the Privacy Act.

33. APP6.2(b).

34. Section 177 of the TIA Act.

So before the 2015 Act providers usually required either:

+ legal compulsion, such as a warrant or other Court order or a statutory notice to produce (like the NSW Crime Commission notice referred to above), or
+ the law enforcement agency to provide a written authorisation under the TIA Act[35] signed by an authorised officer, which notice (if facially valid) exculpates the provider from liability under section 276 for provision of the relevant information about communications as specified in the written authorisation.

Any compulsion to comply with a facially valid authorisation does not flow from the exceptions to section 276 but rather from the vague and controversial section 313 of the Telecommunications Act. This provision requires carriers and CSPs to give Federal and State officers and authorities such help as is reasonably necessary for enforcing the criminal law and laws imposing pecuniary penalties; assisting the enforcement of the criminal laws in force in a foreign country; protecting the public revenue or safeguarding national security. Sections 313(5) and (6) provide a general exculpation from all laws or liability in relation to the provision of such help.

So what limits the scope of an authorisation request? Prior to the 2015 Act entering into operation, section 180F of the TIA Act requires authorised officers of law enforcement agencies, when considering whether to issue an authorisation to disclosure information, to 'have regard to' the impact on an individual's privacy before authorising a service provider to disclose telecommunications data. The 2015 Act amends this section 180F obligation to require authorising officers to "be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate". Authorising officers will also be (newly) required to consider "the gravity of any conduct in relation to which the authorisation is sought, including the seriousness of any offence in relation to which the authorisation is sought, the seriousness of any pecuniary penalty in relation to which the authorisation is sought, and the seriousness of any protection of the public revenue".[36] It remains to be seen whether this will reduce the number of requests for access that appear to relate to relatively minor offences.

The 2015 Act amended the TIA Act to provide that initially only criminal law-enforcement agencies are able to access stored communications (and to require the preservation of stored communications).

Criminal law-enforcement agencies are defined to mean interception agencies (Commonwealth, State and Territory police and anti-corruption agencies) that are able to obtain warrants to intercept communications under the TIA Act; the Australian Customs and Border Protection Service (Customs); the Australian Securities and Investments Commission; the Australian Competition and Consumer Commission; and authorities or bodies declared by the Minister to be a criminal law-enforcement agency. The Minister must not make a declaration unless satisfied on reasonable grounds that the functions of the authority or body include investigating serious contraventions.

However, in relation to information about communications (as distinct from stored communications which reveal the content of communications) section 176A replaced the definition of 'enforcement agency' in the TIA Act with a definition that permits the Minister to declare other authorities and bodies to be 'enforcement agencies' where their functions relevantly include enforcement of the criminal law, administering a law imposing a pecuniary penalty or a law relating to the protection of the public revenue.[37] A relatively extensive list of law-enforcement agencies have now sought to be declared criminal law-enforcement agencies: see the list appended to this paper as released (partially redacted) in January 2916 by the Federal Attorney General in response to a Freedom of Information request.

The 2015 Act does not significantly regulate other or subsequent internal uses of accessed information by law enforcement agencies. Although many submissions to the Parliamentary Committees that considered the 2014 Bill vigorously asserted that such specific regulation was required, these submissions were not taken up in the amendments introduced before the 2014 Bill become the 2015 Act. It was suggested by the Government that such further protections were not required given the operation of the Privacy Act to preclude non-authorised uses, retention or disclosure, regulation of many agencies by their empowering statutes, and other ex post oversight mechanisms. For example, Schedule 3 of the 2015 Act extends the remit of the Ombudsman to enable the Ombudsman to comprehensively assess agency compliance with all of an enforcement agency's (or a criminal law-enforcement agency's) obligations under Chapters 3 and 4 of the TIA Act, including use and access to telecommunications data. Oversight of this category of data would also extend to auditing the use and access to data retained as a result of the data retention obligation.

35. Under a number of provisions of the TIA Act of which the most frequently used are sections 178, 179 and 180.

36. Subparagraph 180F(aa) of the TIA Act.

37. Section 176(1)(3B) of the TIA Act.

OTHER PERSONS THAT MAY ACCESS RETAINED DATA

One criticism of the data retention proposals before the 2015 Act was finalised was that then draft law mandated communications data retention and empowered criminal law enforcement agencies to access that data, but did not limit the circumstances in in which other organisations or individuals might lawfully access that data, such as through exercise of other statutory access powers or through court process such as subpoena or notice to produce. The Parliamentary Joint Committee on Intelligence and Security (PJCIS) received a number of submissions and heard evidence of concerns about a possible increase in the frequency and volume of telecommunications data accessed by civil litigants as a result of the implementation of the data retention scheme and the public interest in confining disclosure of and access to, telecommunications data, to protect the broader privacy interests of the community.

In response to these criticisms a new restriction was inserted into the 2015 Act as enacted. The relevant provision, section 280(1B) of the Telecommunications Act, is obscurely drafted due to multiple levels of double negatives, but the net effect is intended to be that the permission for disclosures or uses as required or authorised by law does not apply where:

- the disclosure is required or authorised because of a subpoena, a notice of disclosure, or an order of a court in connection with a civil proceeding; and
- the disclosure is not to an enforcement agency;
- the information or document is kept by a service provider "solely for the purpose of complying" with the statutory data retention obligation[38]; and
- the information or document is not used or disclosed by the provider for any purpose other than for the specified purposes (such as complying with Part 5-1A or providing individuals with access to their personal information in accordance with the Privacy Act).

Subsections 280(1C) and 281(2) and (3) also contain a regulation making power permitting the Minister administering the Telecommunications Act to prescribe exceptions to this prohibition. This power to make regulations is not circumscribed by the limited period for operation and special Parliamentary oversight provisions that apply to the making of other important regulations under the TIA Act as amended by the 2015 Act. Accordingly, this power would only be subject to the normal disallowance procedures prescribed by the Legislative Instruments Act 2003.[39] The regulation making power will enable the Minister by regulation to bring specified forms of civil litigation outside the prohibition upon disclosure by carriers and CSPs and thereby enable issue of court process issued in the course of that civil litigation for access to retained information.

The Revised Explanatory Memorandum relevantly states:

> This enables exceptions to be formulated with the benefit of, and informed by, detailed empirical information about the use and application of telecommunications data in civil proceedings and enables any anticipated practical impediments to the conduct of litigation to be appropriately addressed. The prohibition on the disclosure of retained data in connection with civil proceedings does not operate in relation to disclosures prior to the data retention scheme being implemented, ensuring the Government has sufficient time to identify and put in place appropriate exceptions.
>
> ....
>
> 404. Paragraph 280(1C)(a) provides that the prohibition contained in subsection 280(1B) does not apply in circumstances of a kind prescribed by the regulations. As noted above, telecommunications data is currently accessed by parties to many civil proceedings, including proceedings relating to international child abduction, family violence, and personal injury or economic harm as a result of negligence or professional malpractice. As the requirement for access depends substantially on the facts and circumstances of each individual civil proceeding, any limit on the availability of such information would have the potential to prejudice the legitimate rights and interests of claimants or respondents in such proceedings. Therefore, a regulation-making power is required to enable the creation of regulations to prescribe further circumstances for where the prohibition in paragraph 280(1B) would not apply.

The data retention scheme was implemented from 13 October 2015. As at March 2016 no regulations had been tabled in the Federal Parliament and accordingly the prohibition in paragraph 280(1B) appears to remain in general operation.

38. Per the Revised Explanatory Memorandum: "401. Telecommunications data that is retained by service providers for their ordinary business purposes or for other regulatory purposes is currently accessed in the course of many civil proceedings. The purpose of paragraph 280(1B)(b) is to ensure that the prohibition applies only to telecommunications data that is collected and retained only for the purpose of complying with Part 5-1A, and that is used by the service provider only for that purpose, a limited range of defined public interest purposes, or for purposes incidental to any of those purposes."

39. Conveniently summarised in The Brief Guide to Senate Procedure No. 19 – Disallowance as available at http://www.aph.gov.au/About_Parliament/Senate/Powers_practice_n_procedures/Brief_Guides_to_Senate_Procedure/No_19.

One practical problem with the operation of these complex provisions may be how to make a determination, if called into question, as to whether a carrier or CSP is collecting or retaining information about communications "solely for the purpose of complying" with the requirements of the TIA Act, or whether such collection or retention may also be for commercial purposes such as data analytics or service quality monitoring and assurance. Of course, the problem might not arise in practice because the carrier or CSP may not elect to oppose the court process. Nonetheless, it is unfortunate that the issue is left for uncertainty and possible disputation, particularly given the potential jeopardy facing the carrier in determining whether to release and potentially be exposed to criminal sanctions in Part 13 of the Telecommunications Act 1997 and also breach of the Privacy Act and clause 4.6.3 of the Telecommunications Consumer Protection Code (C628:2015), or not to release and then possibly be in contempt of court.

LOOKING FORWARD

One principle of judge-developed human rights law is the delightfully named 'equality of arms', which is that each party to legal proceedings must have a reasonable opportunity of presenting their case under conditions that do not disadvantage that party as against other parties to the same proceedings.[40] This principle underlies requirements for discovery and inspection of documents, rights to issue subpoenas and other evidentiary rules designed to enable each party to prepare their case and review relevant material that other parties to that litigation may propose to tender. Prohibiting litigants from accessing telecommunications data as an evidentiary source in civil proceedings potentially reduces the ability of litigants to access a probative source of information relevant (either for or against) their claim or response.

This concern led Patrick Fair of Baker & Mackenzie to write an opinion piece, published in the Australian Financial Review of 23 July 2015 , that was highly critical of the section 280(1B) prohibition. Patrick asserted:

> "Parties to litigation in a civil court are usually able to access evidence that could prove the truth or falsity of facts contested in proceedings. The law requires litigants to make full disclosure of relevant documents. The courts have extensive powers that require litigants and relevant third parties to deliver up evidence. The power exists to help the judge get to the truth. The availability of relevant evidence is critical to the proper administration of justice, being likely to clarify issues in dispute, and may cause a party to settle rather than taking up public resources when the facts are against them. It is not at all clear why it should be assumed that matters being investigated by the police and national security are more important or consequential than every matter that comes before a civil court."

Patrick puts the litigators case well: litigation lawyers like evidence (and lots of it) and they are rightly suspicious of any artificial restriction upon availability of evidence. But there is an alternative view. Subpoenae are issued over the counter by administrative staff in court registries without judicial consideration of their merits.

Fishing expeditions by overly broad subpoena are common. Judicial control is exercised at the 'back end', through consideration of whether to allow into evidence material as subpoenaed, and through an 'implied undertaking' that restricts use of material subpoenaed other than for probative use in the particular litigation. Rights to object to production in response to subpoena often are not exercised. The relevant evidence may be produced because the person subpoenaed (i.e. a communications service provider)

40. As given effect in Article 14 of the International Covenant on Civil and Political Rights. Equality of arms' requires that each party be afforded a reasonable opportunity to present its case under the conditions that do not place it at a substantial disadvantage vis-à-vis another party: Brandstetter v. Austria, Application No: 11170/84; 12876/87; 13468/87, Strasbourg judgment 28 August 1991 §§41-69. Equality of arms' essentially denotes equal procedural ability to state the case.

may have no interest in taking active steps to restrict access, or because the person to whom the communications data relates (and who considers that data sensitive) may or may not be a party to the litigation and aware of the issue of the subpoena.

The Revised Explanatory Memorandum anticipates criticism as to non-compliance with the equality of arms principle and addressed it as follows:

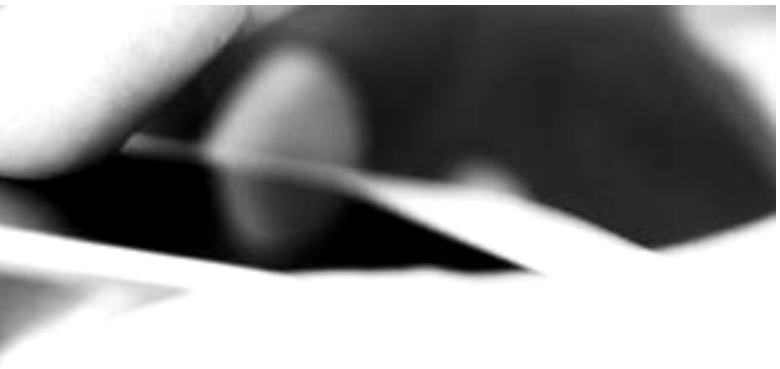
169. However, subsections 280(1B) and 281(2) and (3) do not offend the equality of arms principle as telecommunications data is not be available as an evidentiary source for either party. As such, neither litigant is at a procedural disadvantage in terms of access to evidence or resources to formulate their case. Precluding parties' access to a new source of information does not purport to, nor effectively regulate, the rules of evidence in courts and tribunals or impact the way in which other sources of evidence are collected or presented by either party. The amendments seek to ensure that access to data that is currently available to claimants and respondents is not reduced or limited, as the prohibition is limited to data held solely for the purposes of compliance with the new data retention obligation and related purposes.

171. In summary, none of the fundamental tenets of the right to a fair hearing, including the equality of arms principle are removed, compromised or reduced by the measure. Although the right to a fair hearing is potentially engaged by this measure, it is not limited, in that it would not undermine or compromise the overall procedural efficacy of civil proceedings. The ability of an applicant or plaintiff to present their case or to challenge the case against them is not compromised as the restriction on access to telecommunications data applies equally to both parties. As a result, this measure does not prevent one party accessing their opponent's submissions, nor does it compromise procedural equality or generally restrict access to admissible evidence relied on by the other party or adduced in the proceedings.

It remains to be seen whether (and if so, to what extent) the Minister may by regulation bring specified forms of civil litigation outside the prohibition upon disclosure by carriers and CSPs and thereby enable issue of court process issued in the course of civil litigation for access to retained information. One area of active speculation has been potential use preliminary discovery to access mandatory data sets in support of actions against copyright infringers, such as in the *Dallas Buyers Club* case[41]. In the Victorian, NSW and Federal jurisdictions, preliminary discovery can only be used to obtain information to identify the identity or whereabouts of a prospective defendant or whether or not a cause of action exists. Prior to bringing a preliminary discovery application, parties are required to make reasonable inquiries to attempt to obtain the requested information. *The Dallas Buyers Club* case related to the first category of preliminary discovery – where the party knows they have a claim against certain individuals, however, they do not know the identity of those individuals. Dallas Buyers Club LLC was able to identify 4276 ISP addresses, which were used to share the movie through peer-to-peer networking. However, Dallas Buyers Club LLC did not know any information about the account holders of these ISP addresses. This was the focus of the preliminary discovery application, which was granted by Perram J after extensive analysis of the cases and the basis upon which the judicial discretion should be exercised.

The 2015 Act is legally and technically complex and its operation will be the subject of continuing policy debate. Many critics remain concerned that data retention is mandated at all. Other critics are concerned that the Act is not a proportionate response to threats of terrorism and serious crime, in particular because of limited independent supervision of prospective exercise of the power by law enforcement agencies to authorise access to communications data.

The debate as to communications data retention and access can be expected to continue as the 2015 Act continues to be implemented. The 'internet of things' will continue to increase the range and richness of communications data as well as increase the concerns of many Australian citizens as to how data about them is collected, analysed, used and disclosed. A Brave New World indeed: hopefully not also a foolhardy one.



41. Dallas Buyers Club LLC v iiNet Limited [2015] FCA 317 (7 April 2015) per Perram J, available at http://www.austlii.edu.au/au/cases/cth/FCA/2015/317.html. See also Roads and Traffic Authority of New South Wales v Care Park Pty Ltd [2012] NSWCA 35 and Roads and Traffic Authority (NSW) v Australian National Car Parks Pty Ltd [2007] NSWCA 114. Relevant Court rules include Rule 7.22 of the Federal Court Rules 2011; Court Procedures Rules 2006 (ACT); Rule 5.2, Division 2.8.6, Part 5 UCPRs 2005 (NSW) and Order 32 of the Supreme Court (General Civil Procedure) Rules 2005 (Vic). Order 26A Rules of the Supreme Court (WA).

THE MANDATORY DATA SET		
Topic	Description of information	Explanation
1. The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service	The following: (a) any information that is one or both of the following: i) any name or address information; ii) any other information for identification purposes; relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; (b) any information relating to any contract, agreement or arrangement relating to the relevant account, service or device; (c) any information that is one or both of the following: (i) billing or payment information; (ii) contact information; relating to the relevant service, being information used by the service provider in relation to the relevant service; (d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device; (e) the status of the relevant service or any related account, service or device	This category includes customer identifying details, such as name and address. It also includes contact details, such as phone number and email address. This information allows agencies to confirm a subscriber's identity or link a service or account to a subscriber. This category also includes details about services attached to account, such as the unique identifying number attached to a mobile phone, or the IP address (or addresses) allocated to an internet access account or service. This category further includes billing and payment information. Information about the status of a service can include when an account has been enabled or suspended, a relevant service has been enabled or suspended or is currently roaming, or a telecommunications device has been stolen. The phrases 'any information' and 'any identifiers' should be read to mean the information that the provider obtains or generates that meets the description which follows that phrase. If the provider has no information that meets the description, including because that kind of information does not pertain to the service in question, no information needs to be retained. For instance, if a provider offers a free service and therefore has no billing information, no billing information needs to be retained by that provider with respect to that service the provider will need to retain subscriber and transactional data with respect to that service, but no billing information needs to be retained. Service providers are not required to collect and retain passwords, PINs, secret questions or token codes, which are used for authentication purposes.
2. The source of a communication	Identifiers of a related account, service or device from which a communication has been sent or attempted to be sent by means of the relevant service.	Identifiers for the source of a communication may include, but are not limited to: • the phone number, IMSI, IMEI from which a call or SMS was made • identifying details (such as username, address, number) of the account, service or device from which a text, voice, or multi-media communication was made (examples include email, Voice over IP (VoIP), instant message or video communication) • the IP address and port number allocated to the subscriber or device connected to the internet at the time of the communication, or

THE MANDATORY DATA SET		
Topic	Description of information	Explanation
		• any other service or device identifier known to the provider that uniquely identifies the source of the communication. In all instances, the identifiers retained to identify the source of the communication are the ones relevant to, or used in, the operation of the particular service in question.
3. The destination of a communication	Identifiers of the account, telecommunications device or relevant service to which the communication: a) has been sent; or b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.	Paragraph 187A(4)(b) puts beyond doubt that service providers are not required to keep information about subscribers' web browsing history. The destination of a communication is the recipient. Identifiers for the destination of a communication may include, but are not limited to: • the phone number that received a call or SMS • identifying details (such as username, address or number) of the account, service or device which receives a text, voice or multi-media communication (examples include email, VoIP, instant message or video communication) • the IP address allocated to a subscriber or device connected to the internet at the time of receipt of the communication, or • any other service or device identifier known to the provider that uniquely identifies the destination of the communication. For internet access services, the Bill explicitly excludes anything that is web-browsing history or could amount to web-browsing history, such as a URL or IP address to which a subscriber has browsed. In all instances, the identifiers retained to identify the destination of the communications are the ones relevant to, or used in, the operation of the particular service in question. If the ultimate destination of a communication is not feasibly available to the provider of the service, the provider must retain only the last destination knowable to the provider.
4. The date, time and duration of a communication, or of its connection to a relevant service	The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): a) the start of the communication b) the end of the communication c) the connection to the relevant service, and d) the disconnection from the relevant service.	For phone calls this is simply the time a call started and ended. For internet sessions this is when a device or account connects to a data network and ends when it disconnected – those events may be a few hours to several days, weeks, or longer apart, depending on the design and operation of the service in question.

THE MANDATORY DATA SET		
Topic	Description of information	Explanation
5. The type of a communication and relevant service used in connection with a communication	The following: a) the type of communication; Examples: Voice, SMS, email, chat, forum, social media. b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. c) the features of the relevant service that were, or would have been, used by or enable for the communication. Examples: call waiting, call forwarding, data volume usage.	The type of communication means the form of the communication (for example voice call vs. internet usage). The type of the relevant service (5(b)) provides more technical detail about the service. For example, for a mobile messaging service, whether it is an SMS or MMS. Data volume usage, applicable to internet access services, refers to the amount of data uploaded and downloaded by the subscriber. This information can be measured for each session, or in a way applicable to the operation and billing of the service in question, such as per day or per month. Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c).
6. The location of equipment or a line used in connection with a communication	The following in relation to the equipment or line used to send or receive the communication: a) the location of the equipment or line at the start of the communication; b) the location of the equipment or line at the end of the communication. Examples: Cell towers, Wi-Fi hotspots.	Location records are limited to the location of a device at the start and end of a communication, such as a phone call or Short Message Service (SMS) message. For services provided to a fixed location, such as an ADSL service, this requirement can be met with the retention of the subscriber's address. Paragraph 187A(4)(e) of the Bill provides that location records are limited to information that is used by a service provider in relation to the relevant service. This would include information such as which cell tower, Wi-Fi hotspot or base station a device was connected to at the start and end of communication. Service providers are not required to keep continuous, real-time or precise location records, such as the continuous GPS location of a device. These limitations seek to ensure that the locations records to be kept by service providers do not allow continuous monitoring or tracking of devices.

Available from https://www.ag.gov.au/NationalSecurity/DataRetention/Pages/Default.aspx.

GOVERNMENT ACCESS TO INFORMATION

Per Gizmodo Australia, 18 January 2016

http://www.gizmodo.com.au/2016/01/heres-every-government-agency-that-wants-your-metadata/

In response to a Freedom of Information request, the Australian government has released a partially-redacted list of Commonwealth agencies that have applied for access to the metadata retained by Australia's telecommunications providers as part of the Telecommunications Interception and Access Act. There are over five dozen government entities that want to look through your mobile, internet and home phone records, ostensibly to uncover criminal activity.

Data retention has been in force in Australia since October last year, when the law to enable it passed our Senate by a majority of 43 votes to 16. While telcos are required to store customer data for a minimum of two years for access by registered and sanctioned agencies, there is ongoing confusion over the requirements for that retention.

There are somewhere between 250 and over 500 internet service providers in Australia — the exact number is unknown, as there is no licensing scheme in place or required. Each of those ISPs is required to retain data, but the onus on them to do so is not equal — smaller ISPs bear more financial burden in doing so.

Proper implementation of the data retention scheme even for larger companies is likely at least a year away, according to Internet Australia CEO Laurie Patton. Australia's largest ISP, Telstra, applied for an 18 month extension on the implementation to work out how to integrate such a broad retention scheme into its existing systems.

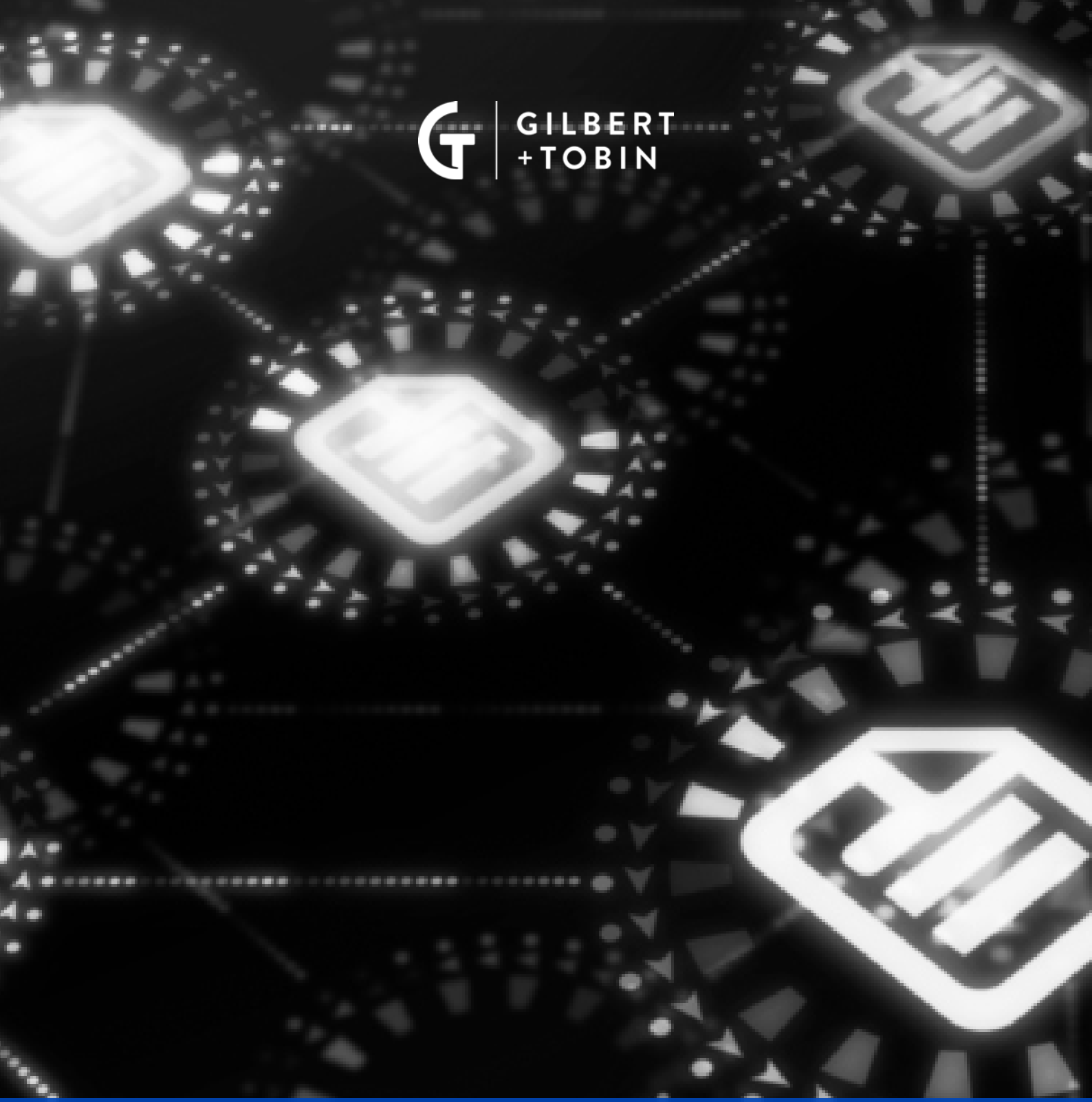
Although the precise nature of Australia's metadata retention is unclear, its thought to extend to telecommunications users' personal details, records of the IP addresses used by their devices, and the broad details of the websites that they access — not the content of the communication itself, but the record that the communication took place. Approved agencies can access stored metadata without having to get a warrant beforehand.

Here's the full list, including the jurisdiction of those agencies:

1. Australian Financial Security Authority, Commonwealth
2. Australian Health Practitioner Regulation Agency (AHPRA), Commonwealth
3. Australian Postal Corporation, Commonwealth
4. Australian Taxation Office, Commonwealth
5. Australian Transaction Reports and Analysis Centre, Commonwealth
6. Civil Aviation, Safety Authority (CASA), Commonwealth
7. Clean Energy Regulator, Commonwealth
8. Department of Agriculture, Commonwealth
9. Department of Defence (ADFIS and IGD), Commonwealth
10. Department of the Environment, Commonwealth
11. Department of Foreign Affairs and Trade, Commonwealth
12. Department of Health, Commonwealth
13. Department of Human Services, Commonwealth
14. Department of Social Services, Commonwealth
15. Fair Work Building and Construction, Commonwealth
16. National Measurement Institute, Commonwealth
17. ACT Revenue Office, ACT
18. Access Canberra (Department of Treasury and Economic Development), ACT
19. Bankstown City Council, NSW
20. Consumer Affairs, VIC
21. Consumer, Building and Occupational Services (Consumer Affairs and Fair Trading – Department of Justice), TAS
22. Consumer and Business Services, SA
23. Department of Agriculture, Fisheries and Forestry, QLD
24. Department of Commerce, WA
25. Department of Corrective Services, WA
26. Department of Environment and Heritage Protection, QLD
27. Department of Economic Development, Jobs, Transport & Resources (Fisheries), VIC
28. Department of Environment, Land, Water and Planning, VIC
29. Department of Environment Regulation, WA
30. Department of Fisheries, WA
31. Department of Justice and Regulation (Consumer Affairs), VIC
32. Department of Justice and Regulation (Sheriff of Victoria), VIC
33. Department of Mines and Petroleum, WA
34. Department of Primary Industries (Fisheries), NSW
35. Environment Protection Authority, SA
36. Greyhound Racing Victoria, VIC
37. Harness Racing New South Wales, NSW
38. Health Care Complaints Commission, NSW
39. Legal Services Board, VIC
40. NSW Environment Protection Authority, NSW
41. NSW Fair Trading, NSW
42. Office of Environment & Heritage, NSW
43. Office of Fair Trading (Department of Justice And Attorney-General Office of the Director General), QLD
44. Office of State Revenue, NSW
45. Office of State Revenue, QLD
46. Office of the Racing Integrity Commissioner, VIC
47. Primary Industries and Regions South Australia (PIRSA), SA
48. Queensland Building and Construction Commission, QLD
49. Racing and Wagering Western Australia, WA
50. Racing NSW, NSW

51. Racing Queensland, QLD
52. Roads and Maritime Serices NSW, NSW
53. Royal Society for the Prevention of Cruelty to Animals (RSPCA), VIC
54. State Revenue Office, VIC
55. Taxi Services Commission, VIC
56. RevenueSA, SA
57. Victorian WorkSafe Authority, VIC

Four agencies have also been redacted from the document under Section 47b as well — their disclosure would be "contrary to the public interest" — for a total of 61 government entities that have applied for ongoing access to the telecommunications data of Australian citizens and residents.



GILBERT
+TOBIN

Sydney
Level 35, Tower 2
International Towers Sydney
200 Barangaroo Avenue
Barangaroo NSW 2000

Melbourne
Level 22, 101 Collins Street
Melbourne VIC 3000

Perth
1202 Hay Street
West Perth WA 6005

GTLAW.COM.AU