Mandatory Internet Data Retention in Australia –
Looking the horse in the mouth after it has bolted

May 2015

Peter Leonard
Gilbert + Tobin and Director, iappANZ
Contents

Introduction 3
Australian telecommunications interception and access law 7
Important trends that led to new data retention laws 10
Who is regulated? Providers of communications carriage services 15
What information must be collected and retained? 19
Data security 22
Who pays? 23
Which agencies or other persons can access retained information? 24
Other persons that may access retained data 28
Looking forward 30
Introduction

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the ‘2014 Bill’) was tabled by the Minister for Communications, The Hon. Malcolm Turnbull MP, in the Australian Parliament on 30 October 2014. The Bill immediately engendered criticism and controversy that continued through its passage through Parliamentary Committees and debates. Notwithstanding those criticisms and a number of critical reports of Parliamentary Committees, the final Act was passed on 26 March 2015 with bipartisan support of the Federal Coalition and Australian Labor Party and assented to on 13 April 2015.

The Bill was enacted as the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (in this article, the ‘2015 Act’) largely as introduced. The 2015 Act principally amends the Telecommunications (Interception and Access) Act 1979 (‘TIA Act’), which continues to operate under that title. The amendments made to the 2014 Bill increased the level of retrospective review as to access to information required to be collected and maintained. The amendments also introduced new provisions to better shield journalists’ sources that might otherwise be revealed through access to communications data and requirements for prior parliamentary scrutiny of any future expansion in the range of service providers that are required to collect and retain data, the categories of data required to be collected and retained by Australian telecommunications service providers and the range of agencies that might exercise powers of access to that data. However, these amendments otherwise did not significantly revise the scope of the requirements to collect and retain relevant data. As a result, Australia now has the most far-reaching data retention requirements among advanced industrialised democracies to collect and retain data imposed upon telecommunications service providers and has the lowest level of independent scrutiny of proposed exercises by enforcement agencies of powers to access that data.

The alleged need for pervasive data collection and retention was stated as arising from new threats of internet facilitated terrorism, child exploitation and human trafficking. These are each very serious crimes that rightly are of priority and focus for Australian intelligence agencies and criminal law enforcement agencies. However, these serious crimes are also not unusually prevalent in Australia. The public testimony of law enforcement officers to the Parliamentary Committees that examined the 2014 Bill did explain why they considered that mandatory data retention would be beneficial to detection and investigation of serious crime, but did not dimension the extent of that benefit nor explain why serious criminals would not avail themselves of anonymisation, encryption and other technologies that would enable them to avoid data surveillance. Schooling as to such evasive techniques is readily available and freely given by many Australian teenagers that use such

---

techniques to evade copyright and parental supervision. A number of senior parliamentarians characterised critics of the Bill as either woolly headed and academic ‘privacy advocates’ who did not understand the ‘real world’ of novel threats and pressing law enforcement needs, or as left leaning lawyers or other civil libertarians who allowed space for criminals to carry out misdeeds and disregarded the rights of Australians ‘with nothing to hide’ to walk down the streets without fear.

In such a climate of polarised debate, it is fair to acknowledge that extensive data collection and retention need not equate to pervasive surveillance and monitoring of individuals. To the extent that Australian official records have been declassified and therefore that recent history is known, the post Cold War history of use of surveillance powers by Australian intelligence and law enforcement agencies has been almost universally benign and uncontroversial. And even enablement of pervasive surveillance does not mean that adverse privacy impacts will necessarily occur – provided, of course, that safeguards are effective to ensure that they do not occur. As well as cultural and behavioural safeguards, categories of possible safeguards include:

- clear definition of and limitation in the scope of what is collected and retained and of the required period of retention
- limitation as to who can access, for what purpose and in what circumstances
- requirements for ex ante (before access) independent review and certification that the access requirements have been met
- retrospective oversight and review, for example, by randomised check audit or other review process
- encryption and security requirements (to ensure that information before access is secured against unauthorised use or disclosure and that information once accessed and in the hands of the agency that accessed that information is also properly protected and secure from unauthorised uses, disclosures or intrusions)
- limitations as to subsequent or collateral access (for example, by court process or other legislative schemes)
- clarity as to collateral constraints (i.e. under general privacy laws)
- transparency and accountability

As discussed later in this article, some of these categories of safeguards were adopted into the 2014 Bill, to varying levels of detail. It was therefore quite easy for Australian parliamentarians to characterise concerns about absence of ‘before the event’ judicial or other independent review of the proposed exercises of access.
powers (as distinct from limited retrospective review by independent oversight bodies), as a ‘rule of law’ excess not required in the liberal and open Australian democracy, where our national culture, as reflected in operating practices of government agencies, naturally protects Australians against the excesses of ‘Stasiland’.\textsuperscript{2} One response might be to note the largely unreported fact that between July 2013 and June 2014 over 550,000 requests for information about communications were made by Australian law enforcement agencies of Australian communications carriers and carriage service providers, and to then query whether that volume of accesses (which surely will substantially rise with much richer data sets retained for two years) will overwhelm any diligent but not liberally funded independent oversight body seeking to identify excessive uses of access powers using check audit methodologies or other sampling techniques. And we do not know how many accesses requests are made by intelligence agencies, because the number of requests is classified. So does Australian culture protect us, or does Australian complacency expose us to administrative excesses? It is interesting that both mainstream media reporting and social media commentary in Australia about the Edward Snowden revelations concerning global surveillance activities by the NSA were each substantially less than in the United States of America and Europe.

In any event, such relatively limited public debate as to the need for impositions of far-reaching telecommunications data retention requirements was not informed by evidence (other than assertions of senior law enforcement and intelligence officials) as to how threats of terrorism, child exploitation and human trafficking would be significantly ameliorated by new communications data retention laws. In the public debate, the fundamental question as to whether collection and retention should be required at all was effectively separated from debate as to who might access retained data and subject to what controls. Concerns as to intrusive or pervasive surveillance was answered by assertions as to the effectiveness of controls as to access. The passage of the legislation was also stated to be urgently required, notwithstanding the fact that the implementation phase timetable for the requirements was 18 months.\textsuperscript{3} Mainstream media attention was fitful and frequently misinformed. Major news media organisations only took an active reporting interest in the Parliamentary debates towards the end of the Parliamentary debates when the media picked up that the data access regime provided no effective ‘shield’ protection of information about journalists interactions with informants such as whistle blowers and no protection for legal professional privilege. Complaints by the Law Council of Australia and other lawyer organisations as to absence of effective protection of legal professional privilege were ignored, but after several weeks of special pleading by the media as to the need for new shield laws for journalists the Government


\textsuperscript{3} Section 187H(2) of the TIA Act as amended defines the ‘implementation phase’ for the purposes of Part 1 of Schedule 1 of the TIA Act as being the period of 18 months starting on the commencement of Part 5-1A.
proposed amendments to the Bill to address this concern.\(^4\) The interest of the media (with the leading exceptions of the ABC and *The Guardian*) then largely evaporated and the 2014 Bill passed as amended.

So now the horse has well and truly bolted, we can ask: have we created a data pool for pervasive surveillance and monitoring of individuals? If so, do we care, or should we be satisfied that the Parliament has limited access to the data pool in such a way that we can be confident that collected and retained telecommunications data will be used sparingly and for proper purposes? To answer these questions first requires a rapid descent into the minutiae of Australian telecommunications law. The answers also require some discussion as to how Australian telecommunications interception and access law developed over time. Once we understand what will be collected and by whom, we can turn to consider the effectiveness of the restrictions upon access to that data.

\(^4\) As now enacted in *Division 4C – Journalists Information Warrants* inserted into the TIA Act by section 6L of the 2015 Act.
Australian telecommunications interception and access law

Australian telecommunications law is rightly seen as an arcane and obscure field of law: relatively recent statute law drafted using technology jargon that despite its youth is usually addressing yesterday’s problem and therefore is not well crafted to address the social concern or business issue of today. At the greatest depths of obscurity lie the laws addressing access to information about communications or (as now notoriously incorrectly described) ‘telecommunications metadata’. 5

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 neither entered the public lexicon nor been declared 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.6 Telephonic communications were protected long before general privacy laws: it was an offence to tap or tape 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 tapping or taping was considered appropriate and hence a judicial warrant was required.7

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 as compared to the warrants regime for interception of call content. By

---


section 177 of the TIA Act and predecessor provisions, a telecommunications carrier 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. By section 178 and related provisions of the TIA Act, an authorised officer of an enforcement agency could give a written authorisation to a carrier which had the effect of mandating provision of information about communications to an authorised officer of that agency, which is purportedly necessary pursuant to enforcement of either 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. In 2012-13 data was accessed by around 80 Commonwealth, State and Territory agencies with law enforcement or revenue protection functions.

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 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. Nonetheless, the number of requests for access steadily grew: between July 2013 and June 2014 over 550,000 requests for information 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 protection of records 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:

---

8 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.
9 Definition of ‘enforcement agency’ in section 5 of the TIA Act as enacted and as amended prior to the 2015 amendments.
10 Revised Explanatory Memorandum, para [10], page 3.
11 Section 178(3) of the TIA Act as enacted and as amended prior to the 2015 amendments.
• 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 is a radical departure from previous law by being the first mechanism to enable preservation 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 Steve Jobs unveiled the iPhone in 2007, he promised: “This will change everything”. Seven years later an estimated two billion people around the globe own a smartphone. In Australia, there are 30 million mobile phones in use for 23 million people and estimates variously are that 60 to 70 percent of all Australians use a smartphone.12

We once lamented that our teenage kids told the story of their lives in their electronic interactions. 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 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 at most hours of the day and are active in various kinds of social media. The digital exhaust of those interactions chronicles each individual’s solitary life and our 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 limits 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. 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. Mandatory data retention funded by the State removes the 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 and facilitate anonymisation and 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 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 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 personable 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.\footnote{OECD Building Blocks for Smart Networks, OECD Digital Economy Papers No. 2015, January 2013.} 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?\footnote{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 Faith Cranor, The Cost of Reading Privacy Policies, at http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.} By 2022 the bathroom and the bedroom will probably remain mute, 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.
<table>
<thead>
<tr>
<th>2012</th>
<th>2017</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 smartphones</td>
<td>4 smartphones</td>
<td>4 smartphones</td>
</tr>
<tr>
<td>2 laptops/computers</td>
<td>2 laptops</td>
<td>2 laptops</td>
</tr>
<tr>
<td>1 tablet</td>
<td>2 tablets</td>
<td>2 tablets</td>
</tr>
<tr>
<td>1 DSL/Cable/Fibre/Wifi Modem</td>
<td>1 connected television</td>
<td>3 connected televisions</td>
</tr>
<tr>
<td>1 printer/scanner</td>
<td>2 connected set-top boxes</td>
<td>3 connected set-top boxes</td>
</tr>
<tr>
<td>1 game console</td>
<td>1 network attached storage</td>
<td>2 e-Readers</td>
</tr>
<tr>
<td></td>
<td>2 e-Readers</td>
<td>1 printer/scanner</td>
</tr>
<tr>
<td></td>
<td>1 printer/scanner</td>
<td>1 smart meter</td>
</tr>
<tr>
<td></td>
<td>1 game console</td>
<td>3 connected stereo systems</td>
</tr>
<tr>
<td></td>
<td>1 smart meter</td>
<td>1 digital camera</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2012</th>
<th>2017</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 connected stereo systems</td>
<td>1 energy consumption display</td>
<td>1 energy consumption display</td>
</tr>
<tr>
<td>1 energy consumption display</td>
<td>2 connected cars</td>
<td>7 smart light bulbs</td>
</tr>
<tr>
<td>1 Internet connection car</td>
<td>3 connected sports devices</td>
<td>1 pair of connected shoes</td>
</tr>
<tr>
<td>1 pay as you drive device</td>
<td>5 internet connected power sockets</td>
<td>1 network storage</td>
</tr>
<tr>
<td>1 network storage</td>
<td>1 weight scale</td>
<td>1 eHealth device</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Pay as you drive devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 intelligent thermostat</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 network attached storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 home automation sensors</td>
</tr>
</tbody>
</table>

**Devices that are likely but not in general use**

<table>
<thead>
<tr>
<th>eReaders</th>
<th>Weight scale</th>
<th>Alarm system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sportsgear</td>
<td>Smart light bulb</td>
<td>In house cameras</td>
</tr>
<tr>
<td>Network attached storage</td>
<td>eHealth monitor</td>
<td>Connected locks</td>
</tr>
<tr>
<td>Connected navigation device</td>
<td>Digital camera</td>
<td></td>
</tr>
<tr>
<td>Set top box</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart meter</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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. Provision of such carriage services to the public 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. 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’). 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 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 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.

---

16 Definition of ‘communications’ and of ‘carriage service’ in section 7 of the Telecommunications Act 1997.
17 Section 42 of the Telecommunications Act 1997.
18 Section 42 of the Telecommunications Act 1997 and definitions of ‘network unit’ in Division 2 of Part 2 of the Telecommunications Act 1997.
19 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 section 16 of that Act.
20 As defined in clause 8 of Schedule 5 to the Broadcasting Services Act 1992.
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\(^{21}\) 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)).\(^{22}\)

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.

For example, section 5 of the TIA Act defines the term ‘carry’ in the same way (being “transmit, switch and receive”) as in the *Telecommunications Act* 1997. However, the addition in section 187A(3)(a) of “enable communications to be carried” is intended, so the Revised Explanatory Memorandum informs us, “to put beyond doubt that data retention obligations apply to relevant services that operate ‘over the top’ of, or in conjunction with, other services that carry communications”.\(^{23}\) Section 187A(4)(c) then excludes from the collection and retention obligation information to the extent that it relates to another service for carrying communications that is “operated by another person using the relevant service operated by the service provider”. A note to that exception as included in the amended TIA Act states that the exception “…puts beyond doubt that service providers are not required to keep information or documents about communications that pass ‘over the top’ of the underlying service they provide, and that are being carried by means of other services operated by other service providers”. The net effect appears intended to be that carriers and ISPs:

---

\(^{21}\) Definition of ‘carrier’ in section 5 of the TIA Act.

\(^{22}\) 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].

\(^{23}\) Revised Explanatory Memorandum at para [227].
• 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.

The next complexity is the carve-down of carriers and ISPs regulated by the Act to only those that operate infrastructure related to the provision of any relevant service in Australia.

The term ‘infrastructure’ is newly defined by subsection 5(1) to mean any line or equipment used to facilitate communications across a telecommunications network. Both ‘equipment’ and ‘line’ are defined using familiar concepts in Australian telecommunications law, ‘equipment’ means apparatus or equipment used in or in connection with a telecommunications network and ‘line’ includes various physical medium used as a continuous artificial guide for or in connection with carrying communications by means of guided electromagnetic energy. Servers used to operate an over the top service such as VoIP are clearly intended to fall within the definition of ‘infrastructure’, while other business operations would not. The Revised Explanatory Memorandum informs us that a piece of equipment or line meeting the definition of infrastructure does not automatically satisfy paragraph 187(3)(c) and states that “a computer used by an employee in a company’s headquarters or marketing office is not directly involved in the provision of a relevant service and therefore does not satisfy paragraph 187(3)(c)“. This appears to be a correct reading of section187(3)(c), but the extended reach of ‘infrastructure’ to capture infrastructure used to operate any ‘relevant service’ in Australia operated by a service provider has potential to sweep into the net of ‘relevant services’ many other services of a service provider that otherwise would not be regulated, merely because (say) the service provider used a server in Australia to operate one of those services. Difficult questions will arise as to when servers are owned and operated by a service provider and as to who operates which elements of a carriage service. For example, some service providers outsource aspects of provision of their services such as mirroring or caching of services or traffic management, or use cloud services providers for particular functions.

The 2015 Act does allow for extensions of the mandatory data collection and retention requirements to other service providers that otherwise would not be caught

24 Definitions of ‘equipment’ and ‘line’ as inserted into amended section 5 of the TIA Act and definition of ‘line’ in section 7 of the Telecommunications Act 1997.
25 Voice over Internet Protocol: Microsoft Skype, Google Voice and Cisco WebEx are examples of VoIP services.
26 Revised Explanatory Memorandum para [420].
within the above scheme. The first is where the Minister declares a service to be within the data retention scheme. Such a declaration ceases to be in force after 40 sitting days of either House of Parliament after the declaration is stated to come into force, thereby enabling a Parliamentary sittings ‘window’ within which an amending bill might be introduced. Subsection 187A(3C) provides that, where a Bill is introduced into the Parliament to amend the classes of service providers to which data retention obligations apply (that is, a bill is introduced that would permanently list an additional class of service provider), the Bill must be referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for inquiry. Subsection 187A(3C) requires the PJCIS to be given a minimum of 15 sitting days of a House of the Parliament for review and report on the bill. An analogous procedure is provided in relation to changes to the data set that is required to be collected and retained.27

Section 187B excludes certain service providers from being required to comply with data retention obligations under subsection 187A(1) of the TIA Act. The stated purpose of section 187B is to ensure that entities such as governments, universities and corporations are not required to retain telecommunications data in relation to their own internal networks (provided these services are not offered to the general public), and that providers of communications services in a single place, such as free Wi-Fi access in cafes and restaurants, are not required to retain telecommunications data in relation to those services. However, the Communications Access Coordinator may declare that data from such services must nevertheless be retained, subject to procedural requirements that do not include a requirement for prior public consultation.

A number of provisions allow for exceptions to be permitted by the Communications Access Coordinator and for data retention plans to be accepted by the Communications Access Coordinator effectively in substitution for compliance with the default statutory obligations. The Revised Explanatory Memorandum provides as an example a situation where the cost of encrypting a legacy system that was not designed to be encrypted would be unduly onerous and the service provider identified alternative information security measures that could be implemented. “However, an exemption would not normally be appropriate where fulfilling the data protection obligations would be merely inconvenient.”28

27 Sections 187AA(2)-(5).
28 Revised Explanatory Memorandum, para [275].
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.29

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.”30 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.31 The kinds of information that a service provider must keep include:32

- 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”;

29 Section 187C.
30 Revised Explanatory Memorandum, para [225].
31 Section 187A(6).
32 Reading together the Table in section 187AA(1) and the Revised Explanatory Memorandum, pages 46 to 50.
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);33

- 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".34 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”.35

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;36

- 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 the service provider only as a result of providing the service.37 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

33 Section 187AA(5).
34 Revised Explanatory Memorandum, para [252], page 49.
35 Section 187A(4)(a), Revised Explanatory Memorandum, para [252], Item 6, page 50.
36 Revised Explanatory Memorandum, para [236], page 42.
37 Section 187A(4)(a), Revised Explanatory Memorandum, paras [240] and [241], page 43.
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”38, 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.

---

38 Section 187A(4)(a), Revised Explanatory Memorandum, para [241], page 43.
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 (C628:2012) 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 1988.39 It also follows that individuals will be able to request access to retained data relating to them (whether or not ‘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.

39 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.
Who pays?

Section 187KB provides legislative authority for the Commonwealth to grant financial assistance to service providers to assist them to comply with obligations imposed by the data retention scheme. The terms and conditions of the financial assistance are to be set out in agreements entered into with service providers on behalf of the Commonwealth.

It remains to be seen which service providers receive financial assistance and in what amounts. As might be expected, the estimates of the financial assistance required vary greatly and are the subject of significant contention.
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”. Disclosure is also permitted where the disclosure “is required or authorised by or under Australian law or a court/tribunal order”. 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”. 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.

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

---

40 Section 16A of the Privacy Act.
41 APP6.2(b).
42 Section 177 of the TIA Act.
• the law enforcement agency to provide a written authorisation under the TIA Act[^43] 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.

For example, the Australian Federal Police (AFP) administers the Access Limitation Scheme which uses section 313 to block domains (websites) which contain the most severe child sexual abuse and exploitation material using the INTERPOL 'Worst of ' child abuse list. When a user seeks to access one of these sites, they are provided a block page that provides certain information, including reasons for the block, and contact details for any dispute about inclusion of the listing on the INTERPOL list. Other agencies, including ASIC, have also in the past used section 313 to prevent the continuing operation of online services in breach or potentially in breach of Australian law (e.g. sites seeking to perpetrate financial fraud).

Section 313 is not amended by the 2015 Act but some of the more expansive applications of section 313 (including in particular an over-blocking by ASIC in an overly broad attempt to block foreign websites offering Australians financial advice) led to an announcement of an Inquiry conducted by the House of Representatives Standing Committee on Infrastructure and Communications. The Committee’s Inquiry Terms of Reference were to examine the use of section 313(3) of the Telecommunications Act 1997 by government agencies to disrupt the operation of illegal online services and as to the most appropriate transparency and accountability measures that should accompany such requests. A final report is to be provided by 1 July 2015.[^44] Although this Inquiry is not directly relevant to the scope and operation of the general exculpation under sections 313(5) and (6) for carriers and CSPs providing (other) help to law enforcement agencies, it is expected that the inquiry may make relevant findings about the operation of section 313.

So a valid authorisation creates legal compulsion to comply with the access request in that authorisation. So what limits the scope of that request? Prior to the 2015 Act entering into operation, section 180F of the TIA Act requires authorised officers of

[^43]: Under a number of provisions of the TIA Act of which the most frequently used are sections 178, 179 and 180.
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 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”. It remains to be seen whether this will reduce the number of
requests for access that appear to relate to relatively minor offences.

Perhaps more significantly, the 2015 Act amends the TIA Act to provide that 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. In
considering whether to make a declaration the Minister must consider several
specified factors including whether the authority or body is required to comply with
the APPs or is required to comply with a binding scheme that protects personal
information or has agreed in writing to comply with a scheme providing such
protection of personal information if a declaration is made.

Section 176A replaces the current definition of ‘enforcement agency’ in the TIA Act
with a definition that limits the authorities and bodies that can access
telecommunications data to criminal law-enforcement agencies and authorities and
bodies declared under section 176A to be an enforcement agency. The currently
open-ended “any body whose functions include administering a law imposing a
pecuniary penalty; or administering a law relating to the protection of the public
revenue”, is replaced with a list of criminal law-enforcement agencies. The Minister
may declare other criminal law-enforcement agencies, but before doing so the
Minister must be satisfied that the authority or body is required to comply with a
binding scheme with the listed privacy-protection mechanisms. The characteristics of
a binding scheme in relation to the protection of personal information must include a

45 Item 6K of the 2014 Act inserting subparagraph 180F(aa) into the TIA Act.
46 Section 110A(3B).
mechanism for monitoring the authority’s or body’s compliance with the scheme and enable individuals to seek recourse if their personal information is mishandled.

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.
Other persons that may access retained data

Another criticism of the data retention requirements was that they mandated communications data retention and empowered criminal law enforcement agencies to access that data, but did not limit ways 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 PJCIS received 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.

Currently, the prohibitions on the disclosure of certain communications-related information and documents under (most relevantly) section 276 of the Telecommunications Act do not apply:

- where the disclosure is in connection with the operation of an enforcement agency within the meaning of the TIA Act, or
- where the disclosure is required or authorised by or under law.\(^47\)

New section 280(1B) of the Telecommunications Act is obscurely drafted due to multiple levels of double negatives, but appears intended to state that paragraph 280(1)(b) does not apply where particular circumstances apply. These circumstances (where disclosure would not be permitted as otherwise required or authorised by or under law) are:

- 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 information or document is kept by a service provider “solely for the purpose of complying” with the statutory data retention obligation; and
- the disclosure sought is not for the purpose of any of: complying with Part 5-1A of the TIA Act (that is, pursuant to the written authorisation procedure above described); complying with the requirements of other warrants or other authorisations under the TIA Act or requests or requirements to make disclosures provided for a limited range of public interest purposes provided for by sections 284 to 288 of the Telecommunications Act (which include using or disclosing data in connection with an emergency warning, a call to an emergency services number, a threat to life situation, or the preservation of human life at sea); providing persons with access to their personal information.

\(^{47}\) Section 280(1)(a) and (b) of the Telecommunications Act.
in accordance with the Privacy Act 1988; a purpose prescribed by the regulations; or a purpose incidental to any of these purposes.

Subsections 280(1B) 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. 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 states that the regulation making provision “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”. It continues: “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.”

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 breach of the Privacy Act, or not to release and then possibly be in contempt of court.


49 Section 187H(2) of the TIA Act as amended by the 2015 Act.
Looking forward

The 2015 Act is legally and technically complex and its operation will be the subject of continuing controversy. Many critics remain concerned that data retention is mandated at all. Other critics will be 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.

It was asserted at the commencement of this paper that Australia now has the most far-reaching data retention requirements to collect and retain data imposed upon telecommunications service providers among advanced industrialised democracies, with the lowest level of independent scrutiny of proposed exercises by enforcement agencies of powers to access communications data. It is possible that other advanced industrialised democracies will now follow Australia’s lead. Until they do, questions will remain as to whether the professed urgency for these measures and lack of independent scrutiny of proposed exercise by enforcement agencies of powers to access that data was either necessary or proportionate. It also remains to be seen whether the Commonwealth Ombudsman and Privacy Commissioner will be adequately resourced to perform their important oversight functions that were key features of the political compromises that enabled this legislation to receive bipartisan support. Only if after the event oversight and public reporting as to that oversight is effective will we know whether law enforcement agencies are appropriately self-regulating in the exercise of their powers to access communications data.

The debate as to communications data retention and access will not end with the enactment and implementation of the 2015 Act. The internet of things and other technological developments 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. Privacy is not dead and pervasive surveillance is facilitated but not mandated or about to become a reality. These are laws for the information-driven society of this new millennium, with all of its promises of benefits through information-driven services and all of its detriments through constantly evolving and expanding challenges to the freedom to live a life without constantly feeling under observation. A *Brave New World* indeed: hopefully not also a foolhardy one.

Peter Leonard

7 May 2015