Privacy Law
Bulletin

Internet data retention in Australia: new controversies and complexities

Peter Leonard *GILBERT + TOBIN*

Takeaway points

- Today there is no specific obligation for Australian communications carriers and carriage service providers to retain either the content of communications, or information about communications, for any particular period.
- The government's proposals for mandatory retention of information about communications — so-called internet "metadata" — for two years will fundamentally change the law and potentially also litigation practice. The outcome of the government's proposed changes is therefore relevant for all lawyers and prospective litigants. Metadata, if retained and available to litigants, could be used to affect the outcome of many civil and criminal cases.
- The effect of the government's proposed changes has not been understood in media commentaries on the new Bill. If the changes are implemented in their current form, the effect will be significantly greater than many commentaries suggest.
- There will be a vociferous debate over the next few months as to whether the government's proposed changes are sufficiently clear and certain, reasonable, necessary and proportionate. That debate is likely to lead to a narrowing of the scope of the Bill and a reduction in reliance upon regulations.

Introduction

Internet data retention is back on the political agenda. The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) was tabled by the Minister for Communications, Malcolm Turnbull MP, in the Australian parliament on 30 October 2014. The controversy started immediately.

Controversy as to the Bill

Same-day media reports suggested that kids accessing pirated movies would be exposed and could be prosecuted by copyright owners that mined this new rich vein of evidentiary material. We then read reports that internet users' private details would be exposed to bad actors that had "one-stop shopping" incentives to hack into "this new honey pot". The Shadow Attorney-General, Mark Dreyfuss MP, responded in more moderate terms:

> This legislation is complex and contentious. It is broader than National Security. It has privacy implications and could also potentially increase the cost of internet bills. It therefore needs to be subject to robust scrutiny over months not weeks.

The federal opposition got its wish: the Bill was referred for review by parliamentary committees. The principal review will be by the Parliamentary Joint Committee on Intelligence and Security. Submissions close on 19 January 2015, with the Committee due to report by 27 February 2015.

The Parliamentary Joint Committee on Human Rights has already reported critically as to the Bill. The Committee recommended that the proposed scheme be sufficiently circumscribed to ensure that limitations on the right to privacy are proportionate (ie, are only as extensive as is strictly necessary). The Committee quoted the European Court of Justice in its ruling in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resource*[1] that such data:

> … taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.

Among other recommendations, the Committee recommended that the Bill be amended to limit disclosure authorisation for data to where it is "necessary" for the investigation of specified serious crimes, or categories of serious crimes. The Committee also suggested that the two-year period for retention be cut down, perhaps to six months. The Committee recommended that the Bill be amended to provide that access to retained data be granted only on the basis of a warrant approved by a

court or independent administrative tribunal. The Senate Standing Committee for the Scrutiny of Bills was also critical, in particular of the "inappropriate delegation of legislative power" and the "insufficiently defined administrative powers" in the Bill's provisions. The Senate Committee recommended a reduction of the scope for regulations under the Bill to change key policy settings, at least without prior review by the parliament.

The Law Council of Australia subsequently voiced similar concerns. The Law Council stated that it accepted that there is a legitimate need for law enforcement and intelligence agencies to have access to telecommunications data. However, it stated that the Law Council did not support a mandatory data retention regime as set out in the Bill because the purpose of mandatory data retention is unclear; blanket mandatory data retention has not been demonstrated as reasonable, necessary or proportionate by the government; the government had not explored (and should explore) less restrictive alternatives that will meet legitimate counter-terrorism purposes; the nature and scope of the data to be retained are unclear, uncertain and subject to change by the Executive (through regulations made under the Act); and the Bill does not provide safeguards or restrictions for civil or for non-law enforcement purposes. "Any mandatory data retention scheme must be shown by the government to be reasonable, necessary and proportionate to a legitimate purpose," said the Council's president, Michael Colbran QC, in a statement.

Cost and who pays

Other criticisms focused on the unverified cost of implementation of data retention, and lack of clarity as to who would bear that cost. When he introduced the Bill on 30 October 2014, the Minister for Communications said that the government "expects to make a substantial contribution to both the cost of implementation and the operation of this scheme", and announced a working group to examine technical and cost issues. However, the extent to which the government will contribute to the financial burden is somewhat unclear. The Attorney-General's Department summarised the government's position by saying that "the government has indicated that it is willing to make a reasonable contribution to the upfront capital costs of the scheme".

As the above quoted reactions to the Bill indicate, data retention debate in Australia will continue to be vociferous and polarising. But at last we have a concrete and public proposal with which to engage. The privacy implications are clearly very significant. This is particularly so because the Bill does little to limit the current broad powers enjoyed by law enforcement agencies to access information about communications. The Bill does propose a default limit of access to a smaller category of such agencies, being "criminal law enforcement agencies", and proposes some new, after-the-event, transparency and accountability measures. However, the broad powers of access remain largely unchanged. Those access powers are also frequently mis-described and misunderstood. So, I will first attempt to explain the Bill in the context of those access powers.

The position today

Presently, there is no specific obligation for Australian communications carriers and carriage service providers to retain either the content of communications, or information about communications, for any particular period

The effect of the Bill (if enacted) would be to create a new obligation to capture and retain for a period of (generally) two years certain categories of information about communications. This information about communications has come (colloquially and misleadingly) to be referred to as "metadata". The retention obligation would be imposed upon most providers of communications carriage services to the public between points within Australia or points within Australia and points outside Australia (international services touching Australia).

We now need to delve into some of the obscurities of telecommunications law to explain why this obligation applies to "most 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 places. *Provision* of such carriage services within Australia using certain types of communications capacity leads to the owner of that capacity — fibre, line or radiocommunications spectrum — being required to be licensed as an Australian telecommunications carrier. *Use* of capacity within Australia, or to and from Australia, to provide such carriage services leads to the provider of such carriage services being a carriage service provider (CSP). CSPs and telecommunications carriers are required to comply with requirements in the Telecommunications Act 997 (Cth) and the Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act). So, an internet access provider — the provider who sells internet access to the householder or business — will usually be a CSP because the provider provides to its customers a service of carriage of traffic over the internet (as well as internet access). An internet service provider (ISP) — not itself a term of art and covering many different types of service providers — may be required to be licensed as a carrier, a CSP or neither. Google, Facebook and Amazon are each ISPs, although their services are quite different from those of internet access providers and other CSPs and telecommunications carriers. iiNet, Optus and Telstra

are carriers as well as ISPs and CSPs. A VoIP provider such as Skype carries voice traffic over the internet and out to non-Skype numbers and so is a CSP. But a provider of cloud services on a "come-to-me" basis — Dropbox, Amazon Web Services and so on — is not a CSP, unless the provider branches out to deliver communications traffic to the public.

Over-the-top services

Many 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, a very important regulatory distinction in most parts of the Telecommunications Act as between carriers and CSPs is collapsed in a few parts of that Act and generally throughout the TIA by deeming provisions that for those parts treat carriage service providers as carriers.

As a result of these confusions and the distortions through layering of many amending Acts, telecommunications has become an arcane byway of Australian regulation, a black art understood by few and feared by many. So, now armed with a working knowledge of the black arts, we are ready to grapple with this Bill.

Infrastructure in Australia

The data retention scheme proposed in the Bill would apply to Australian telecommunications carriers and also to ISPs, including ISPs that are CSPs, but only if they own or operate in Australia infrastructure that enables the provision of any of the provider's relevant services. The Bill provides no guidance as to how to work out whether a person owns or operates in Australia infrastructure that enables the provision of any of the provider's relevant services. This of itself creates real significant uncertainty as to the application of the Bill. Must the "infrastructure" be service delivery infrastructure? If the obligation attaches because a person owns or operates in Australia infrastructure that enables the provision of another, potentially unrelated, "relevant service", how do you determine the limits of application of the provision to other infrastructure?

The scope of "metadata" for retention

This retention obligation would apply to specified information relating to any communication carried by means of the service. The Bill prescribes categories of information that may be required to be retained, but then allows for regulations to be made to specify particular information within these categories that must be retained. So, the Bill would provide the Minister with broad scope, through promulgation of regulations, to prescribe particular information that must be retained. The categories are sufficiently broad to allow prescription of not only much information about communications generated in the course of provision of a CSP's carriage service, but also information relating to use of an OTT application provided by a third party and carried by means of a service provider's service, subject to an exception discussed below. For example, the categories include:

- the characteristics of a subscriber to a relevant service (such as internet access service) using an OTT service (such as name or other identifier, address, billing and payment information);
- information about the source and/or destination of a communication — this category of information may include identifiers used in relation to a VoIP or email service, or any other identifier used to describe a particular OTT service from which a communication originates;
- information about the date, time and duration of a communication, or of its connection to a relevant service — this category may include information about the start and end time of a communication, the carriage of which is enabled by an OTT service provided by a third party;
- information about the type of a communication (such as VoIP, instant messaging or email) provided by a third party OTT provider; and
- the location of equipment used in connection with a communication.

The Bill expressly does not require a service provider to collect and retain:

- the contents or substance of a communication;
- information that states an address (such as IP address, port number or URL) to which a communication was sent on the internet from a telecommunication device using an internet access service provided by the service provider and that was obtained by the service provider "only as a result of providing the service" — this exception is stated as intended to exclude web browsing history from the retention scheme; and
- information if it relates to communications carried by means of an OTT service operated by another service provider — this is a particularly difficult distinction to draw and the Bill provides no real guidance as to how to draw it.

Use of regulations

Draft regulations included for comment in the explanatory memorandum state "kinds of information" within the categories that are proposed to be prescribed by regulation and therefore required to be captured and retained.

Reliance upon regulation-making of itself raises concerns. The making of amendments to an Act of parliament is generally an arduous and drawn-out process involving specialist parliamentary drafters and parliamentary scrutiny before passage. Regulations may be stated to come into immediate effect, albeit then being subject to a requirement for tabling in the next sitting of the parliament and potential disallowance within a limited period by vote of either house. In the sea of legislative rule-making in Australia, parliamentary scrutiny of regulations is often cursory. As a matter of good legislative practice, key matters should be locked down by an Act of parliament.

Regulatory "creep"

There is certain to be lively debate as to whether the categories of information are sufficiently described and circumscribed as to limit regulatory creep through regulations prescribing additional "kinds of information" about communications that must be retained. Regulatory creep might have very substantial financial, as well as privacy, implications: one consequence of prescription of additional kinds of information is likely to be that significant reprogramming or other re-specification of data-capture tools and databases will be required of the affected provider.

So the "kinds of information" (within defined categories) that might be required to be captured and kept are indeterminate, although the government has given us its initial proposal (in the form of a draft regulation). The providers that are required to capture and retain that information are more easily identifiable, although the scope of relevant ISP services is still quite hard to work out. It is not readily apparent how you determine whether a provider owns or operates in Australia "infrastructure that enables" the provision of any of the provider's relevant services. And it is particularly difficult to work out how far the proposed rules are intended to go in relation to capture and retention by underlying CSPs of information about communications using OTT services delivered by other providers over the underlying internet carriage service.

How extensive is the change to retention obligations?

So, how extensive is the change to retention obligations? Well, huge. The TIA (only from October 2012) dealt with preservation of certain "stored communications" (only) "stored" on equipment operated by or in possession of an Australian carrier or CSP, pursuant to:

- a domestic preservation notice, issued by either a law enforcement agency (a broad range of state and federal agencies is listed in s 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 Australian Federal Police following a Mutual Legal Assistance Treaty (MLAT) request made by a foreign law enforcement agency.

The subject matter of the preservation notice is "stored communications", which has been interpreted to mean what is commonly referred to variously as call content, the content of communications or payload data, but not information about communications (ie, service identifiers, device identifiers such as MSISDN, location-related information, date, duration and so on). A domestic preservation notice can only be issued for a 30-day period. It may then be replaced by a telecommunications service warrant — 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. Accordingly, the Bill is the first mechanism to require before-the-event preservation of information about communications on a generic, service-wide basis, not on a case-by-case basis.

Privacy and disclosure

The Privacy Act 1988 (Cth) exempts certain disclosures in permitted general situations as described in s 16A of that Act, including if that 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": Australian Privacy Principle 6.2(b). There are many such laws: various federal, state and territory Acts empower particular agencies to compel disclosure. For example, with regard to the NSW Crime Commission, s 29 (Power to obtain documents and things) of the Crime Commission Act 2012 (NSW) provides that an executive officer 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. Subpoenas are frequently already issued by courts on third parties, including ISPs, to produce records.

Requirements for disclosure

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

Exceptions to s 276 allowed carriers and carriage providers to elect to make voluntary disclosure if "the disclosure is reasonably necessary for the enforcement of the criminal law", "a law imposing a pecuniary penalty or [a law] 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, providers currently usually require either:

- legal compulsion, such as a warrant or other court order or a statutory notice to produce, such as a NSW Crime Commission notice; or
- the law enforcement agency to provide a written authorisation signed by an authorised officer, which (if facially valid) under various provisions exculpates the provider from liability under s 276 for provision of the relevant information about communications as specified in the warrant.

Any compulsion to comply with a facially valid authorisation flows not from the exceptions to s 276, but rather from the vague and controversial s 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. Section 313 then, helpfully for providers, has a general exculpation from all laws or liability in relation to the provision of such help. Some agencies, apparently creatively advised, interpret s 313 as, among other things, enabling them to require blocking of particular internet sites and requiring information about communications to be retained for whatever period they determined. Section 313 is not changed by this Bill and potentially could operate over the newly broadened categories of information to be captured and retained.

Disclosure to whom?

Currently, any federal, state or territory authority or body that enforces a criminal law, a law imposing a pecuniary penalty, or a law that protects the public revenue is an "enforcement agency" under the TIA Act and can seek information about communications under the TIA Act. The Bill would require that bodies that are not a "criminal law enforcement agency" for the purposes of the TIA Act must be declared by the Minister to be an "enforcement agency" before they can authorise the disclosure of information about communications.

The Bill would also amend Ch 3 of the TIA Act to limit the availability of stored communications warrants, authorising access to the content of communications to "criminal law-enforcement agencies". Currently, any authority or body that is an "enforcement agency" can apply for a stored communications warrant.

The Bill would require all Commonwealth, state and territory enforcement agencies to keep specified information and documents in order to demonstrate compliance with their statutory obligations under the proposed scheme. These new record-keeping obligations would expand upon those that currently exist in the TIA Act. The Bill would also give the Commonwealth Ombudsman broad-ranging powers to inspect the records of an enforcement agency so as to assess the extent of its compliance with its obligations relating to the issue of preservation notices and access to stored communications, and access to telecommunications data.

Looking forward

The Bill is complex. Its prospective operation is unlikely to be broadly understood. Many privacy advocates will remain concerned that data retention is mandated at all. Other critics will be concerned that the Bill creates a framework for rules that can be adjusted and expanded through ministerial regulations. Carriers and CSPs will be concerned at the cost of capturing and retaining information and the likely costs of servicing an increasing number of requests for access from law enforcement agencies that can be expected to take advantage of this new evidentiary source.

The data retention debate will not end with this Bill. Rather, the debate has now entered a new phase, possibly just as vociferous and polarising as the debate

before the Bill entered the Australian parliament. As the use of internet devices is now part of everyday life, the tracking of use of multiple internet devices known to be associated with particular individuals provides an ever-richer time-stamped view of that individual's patterns of movement and activity, both within and outside the home. Metadata is not just about with whom individuals communicate. The outcome of the government's proposed changes is therefore relevant for all lawyers and prospective litigants. Metadata, if retained and available to litigants, could be used to affect the outcome of many civil and criminal cases.

Peter Leonard
Partner, Gilbert + Tobin
Board Director, iappANZ
pleonard@gtlaw.com.au
www.gtlaw.com.au

Footnotes

1. *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (C-293/12), judgment of 8 April 2014.