CAMLA COMMUNICATIONS LAW BULLETIN

Communications & Media Law Association Incorporated Volume 34, No 3. November 2015

New Mandatory Data Retention Laws: An Overview

Gordon Hughes and Kanin Lwin provide a high level overview of the new data collection and retention laws and consider its implications on the regulation of personal information under the Privacy Act 1988.

INTRODUCTION

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (***Data Retention Act***) has passed through both Houses of Parliament with bipartisan support. The changes introduced under the Data Retention Act require telecommunications and internet service providers to collect and retain certain types of communications data for a period of two years, unless an appropriate exemption is obtained.

Much of the impetus for introducing this mandatory data retention has been related to national security, with a particular focus on the increasing use of communications technology to carry out criminal or terrorist activity and an alleged lack of available communications data to help authorities investigate and prosecute such activities.

The key provisions in the Data Retention Act commenced in October 2015, although service providers whose data retention implementation plans have been approved by the Communications Access Co-ordinator will effectively receive an additional 18 month window to prepare for the changes.

CHANGES MADE UNDER THE DATA RETENTION ACT

The Data Retention Act largely modifies and develops the existing regime under the *Telecommunications (Interception and Access) Act 1979* (Cth) (***TIAA***). To a lesser extent, the Data Retention Act also amends existing requirements under the *Telecommunications Act 1997* (***Telecommunications Act***) and other legislation such as the *Privacy Act 1988* (Cth) (***Privacy Act***) and the *Intelligence Services Act 2001* (Cth). Chapter 4 of the TIAA already allowed certain authorities to access communications data held by carriers and carriage service providers (***CSPs***) although not the content of those communications. However, prior to the amendments introduced by the Data Retention Act, the TIAA did not specify the types of data which needed to be retained or the period that information needed to be held.

>

CONTENTS

New Mandatory Data Retention Laws: An Overview

Internet of Things - Just Hype or the Next Big Thing?

Profile: Lynette Ireland, Chief General Cousel of Foxtel

Pulp Non-Fiction

SAVE THE DATE - CAMLA AGM and end of year drinks Thursday 19 November

CAMLA Cup 2015 And the winner is...

Valeska Bloch & Victoria Wark

Editorial Board:
Niranjan Arasaratnam
Page Henty
David Rolph
Shane Barber
Lesley Hitchens
Matt Vitins
Deborah Healey
Adam Flynn

Printing & Distribution: BEE Printmail

New Mandatory Data Retention Laws [CONT'D]

> WHO IS REGULATED?

Carriers, CSPs and internet service providers

The Data Retention Act introduces a new section 187A to the TIAA. This provision imposes mandatory data retention obligations on 'carriers', CSPs and 'internet service providers', where they:

(a) **operate** a service for **carrying** communications, or **enabling** communications to be carried, by means of guided or unguided electromagnetic energy; and

(b) own or operate, in Australia, **infrastructure** that enables the provision of **any** of its relevant services.

The Data Retention Act largely modifies and develops the existing regime under the (TIAA)

Although section 187A only expressly refers to carriers and internet service providers, the definition of carrier in the TIAA includes CSPs (except for the purposes of Part 5-4 and Part 5-4A of the TIAA which generally deal with interception capabilities and interception capability plans). The Data Retention Act also permits the Minister, by legislative instrument, to declare that the data retention obligations apply to other specified services as well. At the time of publication, the Attorney-General is the Minister responsible for administering the TIAA.

'Carry'

Section 5 of the TIAA currently defines 'carry' as including transmit, switch and receive.

'Operate'

The term 'operate' is not defined under the Data Retention Act or the TIAA. However, the Explanatory Memorandum interprets the word to at least mean a service is 'operated by' an internet service provider or carrier even if the service itself is not an 'internet access service' (within the meaning of Schedule 5 of the *Broadcasting Services Act 1992*) or a carriage service or a service that would require a carrier license. If this reading is correct, then to take the examples used in the Explanatory Memorandum, if a licensed carrier operates an email service or an internet service provider operates a Voice over Internet Protocol (***VOIP***) telephony service, both services would attract the mandatory data collection and retention obligations notwithstanding that providing an email service does not usually require a licence and that a VOIP service is not itself an internet access service.

'Enable'

Although the new section 187A extends to services that 'enable' the carriage of communications, that term is also undefined. To the extent the interpretation favoured in the Explanatory Memorandum is accurate, the concept of 'enabling' a communication to be carried is intended 'to put beyond doubt' that data retention obligations apply to relevant services that operate 'over the top' of, or in conjunction with, other communication services.

"Over the top of" (***OTT***) services are generally services such as VOIP telephony which are delivered over another underlying internet or telecommunications service that carries the communication, with little or no interaction from the provider of the underlying communication service. The interpretation submitted in the Explanatory Memorandum is presumably in response to previous concerns raised by some enforcement and intelligence agencies that an increasing amount of communications traffic takes place across OTT services, rather than through the traditional communication services previously covered by the TIAA.

'Infrastructure that enables the provision of any of its relevant services'

The Data Retention Act defines 'infrastructure' as meaning any line or equipment used to facilitate communications across a telecommunications network. The words 'line' or 'equipment' are already defined in the TIAA.

However, this does not mean that any equipment or line which satisfies the definition of infrastructure necessarily falls within the scope of the Data Retention Act, since the infrastructure must also enable the provision of the relevant service. The Explanatory Memorandum, for instance, notes that a computer used in a company's headquarters or marketing office is not directly involved in the provision of a service of a kind referred to in section 187A and so would fall outside its scope.

It should be noted that section 187A refers to *'any* of its relevant services' and so could apply to situations where the provider operates a service (for which it does not own or operate any infrastructure in Australia) but also operates another relevant service in relation to which infrastructure is owned or operated within the country. This is the interpretation adopted in the Explanatory Memorandum which states that the intention of section 187A is that the data retention obligation applies, irrespective of whether the person owns or operates infrastructure in Australia relating to the particular service in question.

WHAT ARE THE KEY OBLIGATIONS?

Mandatory data collection and retention

Section 187A requires carriers, CSPs and internet service providers to keep, or cause to be kept, information of the kind specified under section 187AA (or documents containing such data) relating to any communication carried by means of the service. Section 187C imposes a minimum retention period of two years, unless otherwise varied through regulations.

Types of information required to be kept under section 187AA

The Data Retention Act introduced section 187AA into the TIAA, which prescribes the information or documents that a provider must retain and secure to comply with its data retention obligations. Generally speaking, the types of information required to be kept include information about :

(a) the subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service;

(b) the source of a communication;

(c) the destination of a communication;

(d) the date, time and duration of a communication, or of its connection to a relevant service;

(e) the type of a communication or a relevant service used in connection with a communication; and

(f) the location of equipment, or a line, used in connection with a communication.

These categories of information may be amended by an appropriate Ministerial declaration.

Exempted Information

Section 187A(4) however excludes the following types of information from the mandatory data retention obligations:

(a) information that is the contents or substance of a communication;

(b) information that states an address to which a communication was sent on the internet, from a telecommunications device, using an internet access service provided by the service provider and was obtained by the service provider only as a result of providing the service;

(c) information to the extent it relates to a communication carried by means of another service, which leverages the underlying service;

(d) information that a provider is required to delete because of a determination made by ACMA under section 99 of the Telecommunications Act; and

(e) information about the location of a telecommunications device that is not information used by the service provider in relation to the relevant service to which the device is connected.

The Data Retention Act states that these exclusions are intended to place beyond doubt that providers are not required to keep information about telecommunications content, subscribers' web browsing history and 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.

'Communications carried by means of the service'

Sub-section 187A(5) prescribes circumstances in which an attempted or un-tariffed communication constitutes a communication carried be means of the service. These are attempted communications which result in:

(a) a connection between the telecommunications device used in the attempt and another telecommunications device;

(b) an attempted connection between the telecommunications device used in the attempt and another telecommunications device; or

(c) a conclusion being drawn, through the operation of the service, that a connection cannot be made between the telecommunications device used in the attempt and another telecommunication device.

Although the Data Retention Act does not specify what constitutes an 'untariffed communication', the Explanatory Memorandum suggests that this includes 1800 phone calls, communications sent using 'unlimited' phone or internet plans and free internet or application services.

a provider must protect the confidentiality of information that the provider must keep under section 187A by encrypting the information and by protecting the information from unauthorised interference or unauthorised access

Documents not normally created in the course of the service

Sub-section 187A(6) states that, if a provider is required to keep a certain type of information by section 187A, but such information is not created by the operation of the relevant service, the provider must use other means to create the information or a document containing the information.

This obligation is justified under the Explanatory Memorandum as ensuring that a consistent minimum standard is applied across the telecommunications industry for what data is to be collected. The Memorandum also suggests that sub-section 187A(6) applies where information is only created in a transient fashion during the operation of the service, although this is not expressly stated under the Data Retention Act.

Confidentiality and security

The Data Retention Act also imposes obligations to secure communications data once it has been collected and retained. Under the new section 187BA, a provider must protect the confidentiality of information that the provider must keep under section 187A by encrypting the information and by protecting the information from unauthorised interference or unauthorised access. >

> Although encryption is mandated as a method of protection, the level of encryption is not specified under the Data Retention Act meaning this will need to be determined according to the circumstances of each case including, in particular, the technical configuration of the systems used to store information. It should also be noted that section 187BA does not excuse providers from complying with their obligations to disclose information in accordance with a lawful request under the TIAA or the Telecommunications Act. This means that a service provider must not only encrypt the information it is required to collect and retain but must also preserve the technical capability to decrypt and disclose that retained data.

Provisions under the Telecommunications Act currently prohibit the disclosure or use of certain communications information

Communications data as personal information

The security obligations under section 187BA are overlayed by the obligations under Australian Privacy Principle (***APP***) 11.1 of the Privacy Act to reasonably protect personal information from misuse, interference and loss and from unauthorised access or disclosure. Section 187LA states that the Privacy Act applies in relation to a service provider to the extent their activities relate to retained data and that, for the purposes of the Privacy Act, such data is regarded as personal information.

This is significant in that the definition of 'personal information' under section 6 of the Privacy Act is effectively expanded to include any information relating to an individual, regardless of whether (as required by the Privacy Act), the individual is 'reasonably identifiable'.

As section 187LA extends the Privacy Act broadly to all retained communications data, this also means that providers will need to comply with the other non-data security obligations under the APPs such as the requirements governing the cross-border disclosure of personal information and the de-identification and destruction of retained data once ceases to be of relevance.

WHAT SERVICES ARE EXEMPT?

Broadcasting services

The mandatory data retention obligations under section 187A do not apply to broadcasting services, as defined under the *Broadcasting Services Act 1992*. Interestingly, sub-section 187A(3) only expressly excludes broadcasting services and not radiocommunication services. This exemption for radiocommunication services is currently found elsewhere in the TIAA. For instance, the definition of 'telecommunications service' does not include services for carrying communications solely by means of radiocommunication. However, the Explanatory Memorandum notes that this radiocommunication exception is more relevant to situations where it is appropriate to consider the end-to-end passage of a communication across a telecommunications system and that the data retention obligations relate to such parts of the system which may involve a service for carrying communication solely by means of radiocommunication.

'Immediate circle' or 'in the same area' services

Section 187B of the TIAA, as introduced under the Data Retention Act, provides that the data retention obligations do not apply if the services are provided only to a person's 'immediate circle' (within the meaning of section 23 of the Telecommunications Act) or is provided only to places that 'are all in the same area' (within the meaning of section 36 of the Telecommunications Act). This is unless the Communications Access Co-ordinator declares that data from such services must nevertheless be retained.

Services declared by the Co-ordinator

The Communications Access Co-ordinator may also grant exemptions or variations to the obligations imposed on providers under the Data Retention Act. This is intended to introduce flexibility into scheme, such as where imposing a data retention obligation on a service would be of limited utility for law enforcement and security purposes.

Where the Co-ordinator grants a variation, the variation must not impose obligations that would exceed the obligations to which a service provider would otherwise be subject under sub-section 187A(1) and sections 187BA and 187C. These sections generally relate to the collection, retention and protection of communications data.

Services subject to a data retention implementation plan

The Data Retention Act inserts the new sections 187D and 187J into the TIAA, which enable the development of data retention implementation plans. These are, generally speaking, plans which provide a pathway for a provider to become fully compliant with the data retention obligations within an appropriate time period following commencement of the Data Retention Act. A provider must normally apply for approval by the Co-ordinator of their data retention implementation plan.

While a plan is in force, the provider must comply with the plan in relation to communications carried by means of that service in place of the obligations under sub-section 187A(1) and sections 187BA and 187C . These plans will generally remain in force for 18 months after the commencement of the Data Re-

tention Act (if the provider was already operating the service prior to the commencement of the Data Retention Act) or 18 months after the service commences (if the provider begins operating the service after the commencement of the Data Retention Act).

WHO CAN ACCESS THE RETAINED DATA?

Certain entities will be allowed to access communications data, once it has been collected and retained. These include specified enforcement or intelligence agencies and certain civil litigants.

Some current prohibitions

(a) Telecommunications Act prohibitions

Provisions under the Telecommunications Act currently prohibit the disclosure or use of certain communications information. In particular, section 276 prohibits carriers or CSPs from disclosing or using any information or document that relates to the contents or substance of a communication carried by the carrier or CSP which comes into their knowledge/possession in connection with their business as a carrier or CSP.

These prohibitions, in turn, are subject to certain exceptions. For example, section 280 of the Telecommunications Act permits a disclosure or use of information in connection with the operation of an enforcement agency (provided this is authorised under a warrant) or, in any other case, the disclosure or use is required or authorised by law (including subpoenas).

The TIAA also contains some exceptions to section 276 of the Telecommunications Act such as sections 178, 179 and 180 of the TIAA which permit disclosures of information specified in an authorisation issued by an authorised officer of an enforcement agency (eg. the Commissioner of Police) under certain circumstances. Similarly sections 175 and 176 of the TIAA permit disclosures to ASIO in specified instances.

(b) TIAA prohibitions

The TIAA generally makes it an offence to intercept or access communications passing over a telecommunications system. Under section 108, the TIAA also prohibits entities from accessing stored communications, which includes the recording of a communication, where they do so with the knowledge of neither the sender nor intended recipient of the stored communication.

However, sub-section 108(2) exempts carriers and CSPs from stored communications which are accessed under certain types of warrants, such as stored communications warrants.

Enforcement agencies

Although enforcement agencies were already able to access communications information previously, the Data Retention Act has amended the definition of 'enforcement agency' so that it means either a 'criminal law-enforcement agency' or a body which has successfully applied to be included as an enforcement agency.

The list of criminal law enforcement agencies in the Data Retention Act includes many of the agencies previously regarded as enforcement agencies under the TIAA (such as the Australian Federal Police and State police forces). However, it also includes the Australian Customs and Border Protection Service, the Australian Securities and Investments Commission, the Australian Competition and Consumer Commission and any agencies declared by the Minister to be a criminal law-enforcement agency.

With respect to stored communications, the Data Retention Act has amended the TIAA so that (amongst other things) only a criminal law-enforcement agency may apply for a stored communications warrant. The Data Retention Act also inserts a 'proportionality' requirement in respect of disclosures authorised under the TIAA. Previously, under section 180F, the authorised officer considering making the authorisation only considered 'whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable'. The Data Retention Act amends this requirement so that the officer must now be reasonably satisfied that any interference is 'justifiable and proportionate'.

enforcement agencies and ASIO must apply for a "journalist information warrant" before accessing information or documents for the purpose of identifying a journalist's source

Civil Litigants

To address concerns about civil litigants seeking access to a greater amount of communications data as a result of the data retention scheme, the Data Retention Act amends section 280 of the Telecommunications Act so that the permission for disclosures or uses required or authorised by law does not apply where:

(a) the disclosure is required or authorised because of a subpoena, notice of disclosure or a court order in connection with a civil proceeding;

(b) the disclosure is not to an enforcement agency;

(c) the information or document is kept by the provider solely for the purpose of complying with Part 5-1A of the TIAA (as in the mandatory data retention obligations); and

(d) the information or document is not used or disclosed by the provider for any purpose other than for the specified purposes (such as complying with Part 5-1A or providing individuals with access to their personal information in accordance with the Privacy Act).

>

New Mandatory Data Retention Laws [CONT'D]

> These circumstances may be further adjusted via regulation. The amendments do not apply during the implementation phase of the Data Retention Act to ensure that the Commonwealth has adequate time to make any necessary adjustments.

Journalist Information Warrants
Under the amendments to the TIAA, enforcement agencies and ASIO must apply for a "journalist information warrant" before accessing information or documents for the purpose of identifying a journalist's source. There are different procedures for issuing such warrants, depending on whether the applicant is an enforcement agency or ASIO.

(a) Enforcement agency
Where it is an enforcement agency that is seeking the warrant, this is subject to *ex ante* judicial review. Broadly speaking, an application for a warrant will only pass the judicial review if the reviewer is satisfied that the warrant is reasonably necessary to:

(i) enforce the criminal law;

(ii) locate a missing person;

(iii) enforce a law imposing a pecuniary penalty or is for the protection of public revenue; or

(iv) investigate a serious offence or an offence punishable by imprisonment for at least 3 years.

The review must also take into consideration whether the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the journalist's source. The Data Retention Act also creates the role of a "Public Interest Advocate" who may make submissions to the reviewer about matters relevant to whether a warrant should be granted and the conditions attaching to that warrant.

(b) ASIO
Where the Australian Security Intelligence Organisation (***ASIO***) seeks a warrant, this is subject to review by the Minister instead of judicial review. The Minister must nonetheless be satisfied, before issuing the warrant, that identifying the journalist's particular source falls within the scope of ASIO's functions and that the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the source's identity. The "Public Interest Advocate" procedure also applies to warrants sought by ASIO.

However, in certain emergency security situations specified in the new section 180M of the TIAA, ASIO's Director General can issue a journalist information warrant herself/himself and without requiring submissions from the Public Interest Advocate. If the Director General issues the warrant, they must afterwards give a copy of the warrant and the reasons for which it was issued to the Minister and Inspector-General of Intelligence and Security.

The Data Retention Act also prohibits the use or disclosure of certain information about the journalist information warrant (such as whether a warrant has been requested, made or revoked) other than for certain specified purposes such as where disclosure or use is for the purposes of the warrant concerned.

CONCLUSION

The Data Retention Act has introduced a wide array of amendments to the TIAA and Telecommunications Act, in particular by requiring a minimum amount of communications data to be retained. This will have a material impact on telecommunications and internet service providers who may need to adopt new systems and processes to comply with these changes. It remains to be seen whether the increase in costs to the industry, which the Communications Alliance has indicated could exceed $300 million, will be commensurate to the benefits of implementing the data retention scheme.

GORDON HUGHES is a Senior Consultant and KANIN LWIN is a lawyer at Ashurst.

SAVE THE DATE

CAMLA AGM AND END OF YEAR DRINKS

THURSDAY 19TH NOVEMBER