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

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

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

In a two part series James Halliday and Rebekah Lam take a considered look at the phenomenon of, and regulatory and policy issues that apply to, the Internet of Things. In this part they discuss the implications for the communications and content industries including what IoT means for the net neutrality debate in Australia.

There has been a tremendous amount written and discussed about the Internet of Things (IoT). Gartner recently reported that this phenomenon was at the crest of its annual "hype cycle", believing that the development of the IoT is subject to overinflated expectations and that its widespread adoption is still some years away.[1]

Gartner and others attribute this finding in part to a lack of standards between emerging IoT technologies, believing that the work towards common standards will continue for some time. While it is certainly true that a lack of standardisation presents a number of technical challenges in the uptake of the IoT technologies, it also creates unique regulatory challenges.

This article is the first in a two part series examining some of these policy implications in the context of this important emerging technology. In this part we look at some of the implications for the communications and content industries, including what the IoT means for the business models of carriers; interoperability and standards issues; numbering plan and roaming implications; and spectrum allocation policy. We also look at what the IoT means for the net neutrality debate in Australia. In part two, we will examine a range of issues for government and consumers arising out of the IoT.

WHAT IS THE INTERNET OF THINGS?

There is no widely accepted definition of the IoT. It has been variously described as "the third wave of the internet", "a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction" [2], and as "the concept of basically connecting any device with an on and off switch to the internet (and/or to each other").[3] It has also been referred to as "physical objects that connect to the internet through embedded systems and sensors, interacting with it to generate meaningful results and convenience to the end-user community".[4]

The ITU has offered a typically dry definition of the IoT, stating that it is "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[5] The ITU also notes that "through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled." Interestingly, the ITU goes on to say "from a broader perspective, the IoT can be perceived as a vision with technological and societal implications."

There is no widely accepted definition of the IoT.

The inability to clearly articulate exactly what the IoT is and what it encompasses, underlies the complexity generated by its accelerating growth. This growth is producing ever increasing volumes of data, demanding more processing power and requiring more complex analytics. Some predict there will be at least 50 billion connected devices by 2020 (there are currently about three billion) with machine to machine communications generating at least US$900 billion in revenues by that time.[6]

This surge in connected devices is sometimes described as the internet becoming "commoditised" or "industrialised" where the abundance of information about a person's attributes, preferences and behaviour is leading to the "datafication of society"[7]. Data can be captured, analysed and stored by data brokers who provide the information to private companies that use the information for marketing, product development and other business purposes. In this sense then, the IoT is part of a broader trend of big data analytics, which also presents many policy challenges similar to those posed by big data.

What is very clear is that the IoT is not homogeneous but extremely diverse and involves a

>

1 http://www.theguardian.com/technology/2014/aug/12/internet-of-things-most-over-hyped-technology.

2 http://whatis.techtarget.com/definition/Internet-of-Things

3 http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/

4 http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf

5 ITU-T Y.2060 (06/2012) "Overview of the Internet of Things."

6 http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf

range of technologies with a wide array of applications for both individuals and businesses. Some of these technologies exist in industries more regulated than others (e.g. health and transportation) but some industries are not directly regulated by any industry-specific rules (e.g. exercise and diet trackers).

Any regulation of the IoT cannot therefore adopt a "one size fits all" approach but must take into account the complexity of the IoT environment. In some senses, the IoT is a purely incremental issue in the context of broader trends in the communications industry, while in others it also presents its own unique and formidable policy challenges.

It seems then that common standards are still some way off

RISKS AND BENEFITS OF THE IOT

The IoT provides tremendous value to users by offering convenient solutions that not only save time and money, but can also save lives and help governments allocate resources more efficiently. (In common with many other technologies, it also offers endless opportunities for mindless diversion)!

One of the most obvious and immediate challenges arises from the sheer and growing volume of IoT devices. This has many different aspects. Many IoT devices are typically low powered, relatively unsophisticated devices which transmit or receive packets of data intermittently. Individually, each device takes up a miniscule amount of total network capacity; however, together, these devices generate a considerable and growing amount of traffic across mobile and, commonly, fixed (usually via wi-fi) networks. Since this traffic is "device grade", it does not typically require access to consumer grade carriage services to operate. This means that many existing networks may not be optimally engineered for IoT traffic.

The future of the IoT is therefore dependant on robust infrastructure including ubiquitous fit-for-purpose broadband connectivity and sensor based technologies. There is an important practical question about whether these enabling technologies can keep up with the demand to successfully support the growth of the IoT.

As Gartner identifies, one key question is standards. An Intel IoT group senior vice president and general manager recently said, the "IoT is a significant opportunity but one that needs interoperability and scale to fulfil industry predictions of billions of connected devices".[8]

Different vendors are releasing different standards but there is as yet no common or prevailing standard. There are also global initiatives including the Open Interconnect Consortium (OIC). The OIC's purpose is to define a "common communication framework based on industry standard technologies to wirelessly connect and intelligently manage the flow of information among devices, regardless of form factor, operating system or service provider."[9]

OIC is the sponsor for the "IoTivity Project", an open source software framework enabling seamless device-to-device connectivity to address the emerging needs of the IoT. There are also many other standards bodies working on similar or related projects, including the ITU and the European Telecommunications Standards Institute. It seems then that common standards are still some way off.

THE TELECOMMUNICATIONS ACT 1997 (CTH)

In Australia, telecommunications is centrally regulated by the *Telecommunications Act 1997 (Cth)* (**Act**) and related legislation.

Operators of IoT devices will generally not (at least during the early stage of the IoT) be carriers or carriage service providers under the Act because they will not be providing carriage services to the public. In many cases IoT communications will pass over public networks (for example a fixed or cellular network operated by a mobile carrier).

However, experience suggests that over time, IoT operators (government is a possible example in relation to smart cities) may start to deploy their own network units and effectively vertically integrate both carriage and content services. In this case, the operator will become subject to the carrier licensing regime. Alternatively, technology aggregators may bundle and resell carriage services from third party networks to IoT providers, making these aggregators carriage service providers.

IP ADDRESSING ISSUES

There are currently two types of IP addresses in active use: IP version 4 and IP version 6. IPv4 was deployed in 1983 and is still the most commonly used version.[10] Given the numeric basis for IP addresses, Asia, Europe and the US have effectively run out of IPv4 addresses.[11]

IPv6 which has been available since the 1990s caters for trillions of IP addresses and offers more efficient network management, better security and interoperability for mobile networks. However many organisations have been slow in upgrading their hardware for the new version, which creates the risk of disruption as IPv4 addresses become oversubscribed. .[12]

7 Jerome, Joseph, Big Data: Catalyst for a Privacy Conversation, 48 Ind. L. Rev. 213 2014-2015.
8 CommsWire No. 150701, 1 July 2015.
9 http://openinterconnect.org/

There is technical debate about whether IPv6 is an essential precondition to the widespread adoption of the IoT, as some IoT communication models can work within the limitations of the IPv4 model. A plausible outcome would seem to be a progressive migration to IPv6 over time in line with demand for IP identifiers.

ROAMING

Roaming is an inherent issue associated with the IoT since the vast majority of devices and sensors will be mobile and will therefore cross over network boundaries. Domestic roaming is currently not regulated in Australia but governed by inter-carrier agreements. While we do not advocate regulatory intervention in the emerging roaming services market for the IoT, an effective inter-carrier fee structure will be a precursor to the growth of the IoT.

By way of context, the ACCC last looked at whether it should declare mobile domestic inter-carrier roaming services in December 2004.[13] Relevant to its conclusion that it was premature to declare the service was the view that the competition in the market for retail mobile services was not yet fully effective and that there were geographic barriers to achieving nationwide coverage (e.g. availability of spectrum, economies of scale and sunk costs).[14] Similar considerations would seem to apply to IoT related roaming given the early stage of this technology's development.

SPECTRUM ALLOCATION POLICY

Often IoT devices transmit data using a local access technology such as bluetooth or wi-fi. This traffic then transits onto a fixed or, often, a mobile cellular network.

Since there is no national network engineered for low powered devices (such as IoT devices), the increasing amount of traffic already passing through these networks (especially wireless) combined with the likely surge in demand from the IoT adds further demand to the ever increasing need for more mobile bandwidth.

This is a knotty issue. In its recent Five Year Spectrum Outlook 2015-19, the ACMA has said "with the continuing emergence of technologies that rely on the use of spectrum for purposes such as machine-to-machine communications, the Internet of Things (IoT) and digital communications, demand for spectrum continues to grow."[15]

This means not only another demand pressure on mobile carriers for licensed (exclusive use) spectrum, but also creates a policy dilemma in relation to unlicensed (or "class licensed") spectrum which is typically used for local access wireless networks. There is only a limited amount of "class licensed" spectrum for listed purposes including the ISM band.

However, some IoT operators are finding that free "class licensed" spectrum is becoming increasingly cluttered to the point where it is not fit-for-use for their devices, while licensed spectrum is prohibitively expensive.

Thus, for the IoT to be allowed to grow, the ISM band must be sufficiently large and fit-for-purpose to cater for the large number of devices that are likely to use the IoT. This raises important issues about the amount and type of ISM band spectrum which should be allocated for this purpose, and how this should be divided (if at all) between government (and government agencies) and business. In response to the Australian government's "Spectrum Review" (March 2015),[16] the ACMA has recently announced it will adopt the recommendations from the Spectrum Review and is presently considering ways to implement that Review including by creating a more flexible framework for spectrum access to balance the diversity and increasing number of uses and users.[17]

A plausible outcome would seem to be a progressive migration to IPv6 over time in line with demand for IP identifiers

At the same time and in common with its counterparts in the US and Europe, one of the options the ACMA has been reviewing is the concept of spectrum sharing. This could mean that wireless carriers would share spectrum with the federal government or spectrum would be shared on a geographic basis for machine-to-machine technology.

Overall it seems what is required is a mix of spectrum solutions, involving the appropriate mix of access to both licensed and open spectrum.

A LOW POWER WIDE AREA NETWORK FOR AUSTRALIA?

There may in the future be some IoT devices whose social utility justifies installation of dedicated network units to ensure uninterrupted communications. Some examples of this include smart city technology generally, priority assistance services, medical, defence or security applications.

This raises the spectrum issues mentioned above and a policy question for government

>

10 https://www.iana.org/numbers

11 http://au.pcmag.com/internet-products/30648/news/us-to-run-out-of-ipv4-addresses-this-summer

12 http://www.pcmag.com/article2/0,2817,2376887,00.asp

13 http://www.accc.gov.au/system/files/Final%20report%E2%80%94mobile%20domestic%20inter-carrier%20roaming%20service.pdf

14 http://www.accc.gov.au/system/files/Final%20report%E2%80%94mobile%20domestic%20inter-carrier%20roaming%20service.pdf, paragraph 4.5.

15 http://acma.gov.au/~/media/Spectrum%20Transformation%20and%20Government/Issue%20for%20comment/pdf/FYSO%202015-19%20pdf.pdf section 3.3 at page 23.

16 file:///C:/Users/ausjh2/Downloads/Spectrum-Review-report-FINAL_-_for_publishing%20(1).pdf

17 http://www.acma.gov.au/Industry/Spectrum/Spectrum-planning/About-spectrum-planning/acma-welcomes-spectrum-review-recommendations

about the extent to which it should be involved in deployment of such networks. For example, the UK Government chief scientific advisor (Sir Mark Walport) has made a number of policy recommendations in relation to the IoT, including that the UK government investigate whether a stable, low power wide area network be deployed to support existing fibre infrastructure.[18] Some governments have also embraced the concept of the smart city - for example, there are initiatives underway in India, Singapore and China.

It is possible then that the IoT discussion may evolve into a broader debate about whether there should be dedicated IoT networks as this technology matures and develops. This would be certain to raise similar issues around the current NBN debate such as cost, deployment, structure and policy framework (including competition issues).

an effective inter-carrier fee structure will be a precursor to the growth of the IoT

NET NEUTRALITY

As the IoT develops and involves increasing amounts of data, networks risk becoming congested. This raises the question of whether some data flows should be prioritised over others. For example, should data associated with health monitoring devices such as heart rate monitors or glucose readings should take priority over data flows updating a user's calorie intake.

The Internet is broadly based on the principle of net neutrality which requires there be an open Internet that allows users to go where they want, when they want. In support of this principle, in February 2015, the US Federal Communications Commission (**FCC**) adopted a set of Open Internet rules which seek to protect and maintain open, uninhibited access to legal, online content and prohibit ISPs from being allowed to block, impair or establish fast/slow lanes to lawful content.[19]

There is no equivalent rule in Australia, although there is a telecommunications interconnection access regime for declared services which is administered by the ACCC. This regime aims to facilitate third party access to certain services to promote the economically efficient operation and use of investment in infrastructure, and promote the effective competition in upstream and downstream markets. The declared services regime does not currently impose net neutrality rules on Australian carriers.

In contrast, the US FCC Open Internet rules apply to both fixed and mobile broadband services and involve three key principles:

1. no blocking - ISPs must not block access to legal content, applications, services or non-harmful devices;
2. no throttling - ISPs must not impair or degrade lawful internet traffic on the basis of content, applications, services or non-harmful devices; and
3. no paid prioritisation - ISPs must not favour some lawful internet traffic over other lawful traffic in exchange for consideration of any kind (including from their affiliates).

The FCC has taken the position that bandwidth services are considered utilities (like water and gas) and therefore subject to considerable regulatory restrictions. These restrictions prevent ISPs from requesting additional fees for faster connection services or for blocking some types of content. Complaints for overcharging are investigated by the FCC.

The Open Internet rules do not yet have any specific IoT parameters. So it is uncertain how they would apply to situations where there may be a legitimate reason to prioritise certain enterprise traffic over others e.g. health monitoring applications or public safety applications or to de-prioritise certain non-essential services when traffic is congested.

CONCLUSIONS

This short overview has shown the many issues emerging from the IoT. Governments around the world have been somewhat active in addressing these issues. For example, the European Union considers the IoT an essential part of its Digital Agenda for Europe 2020; other sovereign initiatives are described above.

To some extent in Australia the legal and policy response to the IoT continues to be a work in progress. The response is informed by the international developments mentioned above as well as the unique challenges of the Australian communications environment. What is clear is that the IoT presents a range of complex and inter-related policy issues which will become only more pronounced as this technology matures.

In part two to be published in the final edition of the CAMLA Bulletin of 2015 we will consider issues arising out of the IoT that are unique for government and consumers.

JAMES HALLIDAY is a partner and REBEKAH LAW is an associate in the corporate group at Baker McKenzie in Sydney.

This article represents the personal view of the authors and is not necessarily representative of the views of any client of the firm.

18 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf ; recommendation 4a.

19 https://www.fcc.gov/openinternet

Profile: Lynette Ireland

Chief General Counsel of Foxtel

CAMLA Young Lawyers representative, Maggie Chan, recently caught up with Lynette Ireland, Chief General Counsel of Foxtel, to discuss her role at Australia's largest subscription television operator, and her views on the key issues facing the industry.

1. *How and where did your career start?*

I started as a junior lawyer at Allens. I was originally in the Trade and Resources area (mining and trade practices) and then I rotated into a general corporate commercial area that included film and television. I was also doing volunteer work at the Arts Law Centre and trying to do as much film work as possible.

At the end of my second year at Allens I was offered a secondment to the Australian Film Finance Corporation (now Screen Australia) for a few months. I really enjoyed my time at Screen Australia and it gave me my first taste for working in-house. I worked as part of a small legal team that was supported by a number of external law firms including Allens. It was very fast moving and I enjoyed working closely with the commercial teams.

This opportunity really helped me when I went back to Allens as it made me better appreciate the issues that are important to clients. I was offered another secondment, this time with Foxtel. Foxtel proved to be very addictive and I knew at the end of the 12 months that I really wanted to stay. Twenty years later, I am still here! I have been lucky that new opportunities have opened up for me at the right time. When I first moved to Foxtel, I was a 3 PAE lawyer. I became Senior Legal Counsel after another 3 years and then General Counsel a few years after that.

2. *What is the scope of your role and your major responsibilities?*

I manage the lawyers and the classification team within Foxtel. The legal team has an incredibly broad brief and we cover all areas from broadcasting, telecommunications and technology, general commercial, intellectual property, competition, company secretarial, employment and work health and safety. The classification team is responsible for the classification of all programming that is broadcast by the Foxtel produced channels.

I am also part of the Foxtel Executive team and I sit on a number of boards including the industry organisation, ASTRA and the Intellectual Property Awareness Foundation.

3. *How big is the team you manage and how is the work organised?*

I manage a team of 27 people and everyone is essentially allocated to a particular stream. Those streams are compliance and regulatory; telecommunications; engineering, information technology and marketing; programme acquisitions and production; channels and wholesale; and classification.

While the team is organised in this way to help the business and manage workloads, I am a big believer in working across the teams. This allows people to build up their skill base and get to know other areas of the business.

4. *What are some of the most interesting and challenging aspects of your role?*

As part of the Executive team and a participant in board meetings I am very involved in business strategy in addition to the legal function. This has the benefit of ensuring that I can better anticipate legal issues and en-

sure that the business appreciates any risk that may be associated with a particular course of action.

My main clients are the CEO and other Foxtel Executives, so I need to be fast-thinking. One of the benefits of being there for so long is that I know how the business works and this allows me to provide a better service to the business.

5. *In your opinion, what are the biggest legal issues facing the broadcasting and media industry in the next 2 years?*

I think one of the biggest legal issues facing our industry is the growth of online piracy and the extent to which people are illegally downloading content.

The new Copyright Amendment (Online Infringement) Act 2015 should assist in reducing access by Australians to sites such as The Pirate Bay. Similar legislation exists in a number of other jurisdictions including the UK and there is evidence from those jurisdictions that injunctions blocking access to sites that are primarily intended to provide illegal access to programming and music do reduce traffic to those sites.

I'm hoping that this is something that rights holders will make use of soon. As a subscription business, we need to try to manage online piracy but also educate people about legal options available to access content.

We are also working with ISPs to introduce a notice scheme that should also assist in educating Australians about legal options for accessing content. We hope that the combination of these 2 things together with the continuing availability of great affordable content will help to reduce the current levels of piracy.

I also think the issue of data management is going to become even more significant for media businesses over the next few years as the opportunities for digital transactions continue to grow. Being able to harness the wealth of data within our business to improve our services while continuing to meet the privacy expectations of our customers is a growing challenge for us, as it is for all digital businesses. What you love to watch can say a lot about you! It is our job to treat this information with respect but also use it to provide you with a better entertainment experience.

6. *How has Foxtel dealt with the rise of digital content and in particular online subscription providers such as Netflix in Australia? Has this made negotiations regarding content exclusivity more difficult?*

Foxtel significantly reduced the price of our entry level product in 2014 from $50 to $25. We have also changed the way we package our products and have given existing customers additional content as a reward for loyalty.

We also launched Presto which, like Netflix, is a streaming subscription video on demand service. We initially launched with Presto Movies and then entered into a joint venture with the Seven Network to produce a general entertainment offering known as Presto Television which compliments Presto Movies. Customers can buy either product separately or as a bundle.

Presto uses subscription video on demand rights (ie SVOD rights) and those rights were often bundled in with the linear rights years ago. The main value used to be put on the ability to broadcast a particular programme as part of a linear service. However SVOD rights now have a price of their own and there is a lot of competition for key titles.

Services like Netflix and Presto, contain a lot of library content supplemented by tent poles which are the hook for these services. The negotiations for these titles have become incredibly competitive.

7. *Having worked in both private practice and in-house, what do you think are the key differences?*

In private practice, the client is more removed and you have multiple clients. You can obviously still have a very close relationship with your clients however *as an in-house lawyer, your client is typically standing in your office or waiting outside to talk to you.*

8. *What skills and attributes do you look for in junior lawyers wanting to join your team?*

I look for people who are enthusiastic about joining Foxtel. I love to see skills that are relevant to a particular position, but if I am choosing between 2 candidates and one has shown real enthusiasm for Foxtel and an understanding of our business then that usually weighs in their favour.

Good communication skills and being able to adapt are also important. For example, some clients in-house want an answer, whereas other want an analysis. You need to be perceptive about what your client wants.

The Foxtel in-house team is very much a mix as to where people have come from. We have a couple of graduates straight from uni, some lawyers from private practice and some lawyers from other in-house roles.

9. *What advice do you have for young lawyers who would like to pursue an in-house role in the media industry?*

People shouldn't hesitate to be proactive. Don't feel like there has to be a role advertised to make an approach. Most businesses have HR teams where they keep CV databases. They may not have a role immediately but one may come up in the future and I like to reward that initiative.

I also think volunteering is a great way to build up your skill base and I know the Arts Law centre, for example, really appreciates volunteers.

MAGGIE CHAN
Maggie Chan is a lawyer in Sydney at King & Wood Mallesons.

IF YOU WOULD LIKE TO SUGGEST SOMEONE TO BE INTERVIEWED BY THE CLB, PLEASE SEND AN EMAIL TO THE EDITORS AT EDITOR@CAMLA.ORG.AU.

CAMLA CUP 2015
AND THE WINNER IS...

CONGRATULATIONS TO WEBB HENDERSON WHO TOOK OUT THE 2015 CAMLA CUP TRIVIA NIGHT. A SPECIAL MENTION GOES TO CLAYTON UTZ COMING IN FOURTH AND ALSO WINNING TWO TABLE QUIZ PRIZES.

WE ALWAYS HAVE A BALL THANKS TO OUR WONDERFUL MC AND QUIZ MASTER, DEBRA RICHARDS. RYAN GRANT MADE AN EXCELLENT 'SOUS MC' AND A BIG THANKS TO RAESHELL TANG FOR WARMLY MEETING, GREETING AND SEATING OUR TEAMS.

THE CAMLA CUP WOULD NOT BE POSSIBLE WITHOUT THE GENEROUS DONATIONS FROM OUR SPONSORS.

THE PRIZES WERE AMAZING THIS YEAR AND WE'D LIKE TO THANK GULLEY SHIMELD FOR TAKING CARE OF THE LOOT AHEAD OF THE NIGHT.

A VERY BIG THANKS FROM CAMLA TO:

ALLENS
ASHURST
AUSFILM
BAKER & MCKENZIE
BANKI HADDOCK FIORA
BIRD & BIRD
CLAYTON UTZ
COPYRIGHT AGENCY
CORRS CHAMBERS
WESTGARTH
FOXTEL
FREE TV
HENRY DAVIS YORK
HOLDING REDLICH
IICA
MINTER ELLISON
NETWORK TEN
NEWS CORP
NORTHERN PICTURES/ RACAT GROUP
NORTON ROSE FULBRIGHT
PAN MACMILLAN
SAINTY LAW
SBS
UNSW
WEBB HENDERSON
YAHOO!7

CAMLA LOOKS FORWARD TO CONTINUING THIS FINE TRADITION NEXT YEAR.

Pulp Non-Fiction

Publishers, pulping and religious insult in India: this paper considers the fraught balance between freedom of speech and sensitivity to religious defamation in India, based on a case study of the legal controversy surrounding the publication of Wendy Doniger's 2010 book 'The Hindus: An Alternative History.'

INTRODUCTION

India is a nation flush with religious diversity, an eclectic mix which has often posed a political problem for this young democracy. The desire to shield the sacrosanct and private right to practice one's faith is at constant war with a constitutional largesse that prohibits unreasonable interference with free speech.[1] In the same breath, the constitution carves out a specific exception for defamation. If navigating these lines between belief, speech and insult is a problem for those who govern, it is an equally frustrating dance for writers and publishers.

Widespread acts of protest on social media suggested that Penguin ought to change its logo to a chicken

This paper explores how publishers manage the risk of legal and reputational liability in this environment by tracking the scandal surrounding Wendy Doniger's book, *The Hindus: An Alternative History*, (***The Hindus***)[2] After a four-year legal battle, in February 2014 Penguin Books India consented to pulp all remaining copies of the controversial book to settle two criminal complaints and a civil suit filed by Dinanath Batra on behalf of activist group Shiksha Bachao Andolan (***SBA***).[3]

While Penguin refused to disclose reasons for the move, the measure appeared politically and commercially defensible. Withdrawal from the Indian market allowed Penguin to generate internet and foreign sales. Against the background of national elections where talks of culture wars were rife,[4] the prospect of a public lawsuit was unsavoury. The publisher's reputation is, after all, as much on trial as that of the plaintiff; and this provocation was nothing if not profitable. But as other Doniger books threatened to disappear from the shelves, Penguin may have deterred legal confrontation at the cost of setting dangerous precedent on the politics of cultural regulation.

FILTHY PAGANISM: THE TEXT AND THE SCANDAL

Wendy Doniger is a well-known Indologist at the University of Chicago. Known for her vivid and wickedly droll prose, she is no stranger to controversy. As a philologist, Doniger's work naturally encounters the pleasures and pitfalls of language and history. The politics of writing religion are often dealt with subtly in scholarship, but Doniger openly departs from this trend:

> "...most non-Hindu scholars of Hinduism strike the familiar religious studies yoga posture of leaning over backward, in their attempt to avoid offense to the people they write about...the Sanskrit texts were written at a time of glorious sexual openness and insight, and I have often focused on precisely those parts of the texts."[5]

But her studies of Hinduism's alterity have rarely drawn this level of notoriety. In 2010, her alternative history of Hinduism in *The Hindus* finally proved too 'sexy' for SBA's Dinanath Batra when the Indian edition was released by Penguin Books India.

Her self-confessed intention to move away from attempts 'to avoid offense to the people [non-Hindu scholars] write about', is exactly as her accusers describe. On 3 March 2010, SBA served a prolix legal notice[6] on Doniger and Penguin alleging the entire publication was coloured by perversity, attracting contraventions of sections 153, 153A, 295A, 298 and 505(2) of the Indian Penal Code (***IPC***). These provisions are concerned with the criminalisation of various forms of religious and cultural hate-speech (discussed later under para [4]). The tome was perceived to be 'riddled with heresies and factual inaccuracies',[7] blindly spreading 'pornography and hate

1 *Constitution of India* art 19.

2 Wendy Doniger, *The Hindus: An Alternative History* (Penguin, 2009) 26.

3 'Penguin India's Statement on 'The Hindus' by Wendy Doniger', *Penguin India* (online), February 2014 <http://www.penguinbooksindia.com/en/content/penguin-india%E2%80%99s-statement-%E2%80%98-hindus%E2%80%99-wendy-doniger>.

4 See for example: Rohan Kalyan, 'Did India Just Elect Its Ronald Reagan?' *Economic and Political Weekly* (online) 31 May 2014 <http://www.epw.in/web-exclusives/did-india-just-elect-its-ronald-reagan.html>.

5 Doniger, above n 2, 21.

6 Full text reproduced on *Outlook Magazine* (online) 11 February 2014 <http://www.outlookindia.com/article/your-approach-is-that-of-a-woman-hungry-of-sex/289468>.

7 Shougat Dasgupta, 'Penguin India settles a civil suit with Dinanath Batra over Wendy Doniger's controversial book on Hinduism', *Live Mint & the Wall Street Journal* (online), 12 February 2014 <http://www.livemint.com/Specials/ZL8MkEyTobNWPEQm05jYDL/Dinanath-Batra-Here-comes-the-book-police.html>.

literature'. Civil and criminal complaints were filed. After simmering in the courts for over three years, in February 2014 Penguin settled on terms that it would withdraw the book from the market in exchange for SBA dropping all pending complaints and lawsuits. A ream of alleged settlement documents were quickly leaked online.[8]

With a provocative private act of management, did Penguin barter moral triumph for discretion and temporary commercial gain?

MORAL PANIC: THE PUBLIC TEMPER

Public responses to the settlement were swift and critical. Numerous articles lamented the pulping of 'liberal India'[9] and expressed dissatisfaction with the impact of private bargains on the conditions of treasured public freedoms.[10] Widespread acts of protest on social media[11] suggested that Penguin ought to change its logo to a chicken.[12] . Downloadable copies of *The Hindus* were quickly circulated online – technology and human effort combined to defeat the letter of a private undertaking. On Amazon.com as of 11 February 2014, there were only two copies of the book left in stock.[13] Three days later it slotted in at number 26 on the Amazon top-seller list.[14]

Politics featured prominently in the discourse around the book, against a background of culture wars and a historic election that eventually landed a significant victory for the 'right-wing' Bharatiya Janata Party (***BJP***). Journalist Sunny Hundal argued that the withdrawal of Doniger's book was not unrelated to the BJP's recent successes. He noted that in the same week, the USA ended its boycott of the then BJP prime ministerial candidate, Narendra Modi. Modi's visa had previously been cancelled for alleged violations of religious freedom.[15] SBA itself appears committed to endorsing a particular understanding of Hinduism in India. This brand of nationalism is termed, not without passionate objection, 'Hindutva'.

From a regulatory standpoint, a string of events and decisions have contributed to a perceived turn against freedom of speech in India. According to one study, India is the second largest issuer of take-down notices to Google, mostly for material that may cause religious offence (55% of requests).[16] Recent defamation cases had also set an unfavourable tone.[17] Moreover, Modi was Chief Minister of the state of Gujarat when it banned a biography of Mohandas Gandhi which suggested that the iconic man "was bisexual".[18]

According to one study, India is the second largest issuer of take-down notices to Google, mostly for material that may cause religious offence (55% of requests)

It is no surprise then that *The Hindus* could well constitute grounds for state censorship. For example in one particular passage, Doniger writes Gandhi had a "habit of sleeping beside girls young enough to be called jailbait in the United States, to test...his celibate control".[19] In 2006, the eminent artist M.F Husain resigned himself to exile after receiving death threats from nationalist groups for 'obscene' works, namely paintings of deities in the nude.[20] On this example Doniger's book jacket, stamped with frolicking deities, invites trouble.

Despite the moral panic organised around pulping, nary a book nor leaf of paper was reportedly harmed in the end. By May 2014, all extant copies of the book had sold out.[21] Yet the discourse remains haunted by a sense of loss. As James Raven explains, there

>

8 'Penguin India Withdrawn Copies of Wendy Doniger's Controversial Book The Hindus' *The Economic Times* (online) 12 February 2014 < http://articles.economictimes.indiatimes.com/2014-02-12/news/47269928_1_publishers-controversial-book-penguin-india>.

9 Sunny Hundal, 'The pulping of liberal India' *The Independent* (online), 27 February 2014 <http://ezproxy.library.usyd.edu.au/login?url=http://search.proquest.com/docview/1502086503?accountid=14757>.

10 See for example: Krista Mahr, 'Penguin India to Recall and Destroy Renowned American Scholar's Book on Hinduism' *Time.com* (online), 18 February 2014 <http://web.a.ebscohost.com.ezproxy1.library.usyd.edu.au/bsi/detail?sid=9fbde422-a62d-4805-8542-18c1907e1aaa%40sessionmgr4001&vid=1&hid=4204&bd>.

11 See: Ananya Vajpeyi, 'Reconsider and Revise Sections 153(A) and 295(A) of the Indian Penal Code to Protect Freedom of Expression in India!' (online) <https://www.change.org/en-IN/petitions/members-of-both-houses-of-the-indian-parliament-and-the-honorable-law-minister-government-of-india-reconsider-and-revise-sections-153-a-and-295-a-of-the-indian-penal-code-to-protect-freedom-of-expression-in-india>; Alison Flood, 'Penguin India Faces Growing Protests Over Withdrawal of Hinduism History,' (online) 19 February 2014 <http://www.theguardian.com/books/2014/feb/19/penguin-india-protest-hindus-wendy-doniger>.

12 'The Penguin is Mutating into a Chicken' *Outlook* (online), 14 February 2014 <http://www.outlookindia.com/article.aspx?289534>.

13 Kian Ganz, "Penguin Settles Religious Conservatives' Civil and Criminal Cases by Pulping Book of Hindu History," *Legally India* (online), 11 February 2014 <http://www.legallyindia.com/201402114335/Bar-Bench-Litigation/penguin-pulps-hindu-book>.

14 Jonah Tabb, "Penguin India Bans University Professor's Book," *The Chicago Maroon* (online), 14 February 2014 <http://chicagomaroon.com/2014/02/14/penguin-india-bans-university-professors-book/>

15 Hundal, above n 9.

16 Jane Bambauer and Derek Bambauer, 'Vanished' (2013) 18 *Virginia Journal of Law and Technology* 137, 137, 142, 150.

17 Ellen Barry, 'Indian Publisher Withdraws Book, Stoking Fears of Nationalist Pressure' *New York Times* (online), 13 February 2013 <http://www.nytimes.com/2014/02/15/world/asia/indian-publisher-withdraws-book-stoking-fears-of-nationalist-pressure.html>.

18 Shashank Bengali, 'India's Tough Defamation Laws Put Book Publishers in a Bind' *South Florida Sun-Sentinel* (online), 27 February 2014 <http://ezproxy.library.usyd.edu.au/login?url=http://search.proquest.com/docview/1507675874?accountid=14757>.

19 Doniger, above n 2, 402.

20 He remained as such until his death, despite court orders quashing orders of his arrest: *Maqbool Fida Hussain v Raj Kumar Pandey* (2008) Crim L J (Delhi HC) 4107.

21 Wendy Doniger, 'India: Censorship by the Batra Brigade' *New York Review of Books* (online) 8 May 2014 <http://www.nybooks.com/articles/archives/2014/may/08/india-censorship-batra-brigade/>.

Pulp Non-Fiction [CONT'D]

> is a strong cultural preoccupation with the 'vanishment' of literary forms.[22] The spectre of loss, real or imagined, is deeply affective in a nation whose history has been marked by colonial experiences of cultural destruction and censorship.

the concept of 'group defamation' has found expression in the IPC as a means of identifying, criminalising and punishing forms of conduct and speech thought to be "inimical" to the public interest

COULD PENGUIN HAVE 'WON'?

There are competing viewpoints around the vexed question of legal victory for Penguin under the IPC. Some legal experts suggest the law is doctrinally indeterminate,[23] while others believe academic dissent would not have come within the punishable ambit of the law.[24] Indeed, veteran lawyer and author A G Noorani persuasively argued that the relevant provisions of the IPC would not have applied at all.[25]

Two key criminal complaints were aired against the publisher and author, though its precise contents remain mysterious. Little known is that the criminal contraventions recited in the legal notice to Penguin apparently did not register as First Information Reports (FIR) (which ordinarily initiate investigations under the IPC).[26] In theory however, state criminal procedure codes empower governments to order the forfeiture of impugned publications, judged on the standards of 'reasonable, strong-minded, firm and courageous'[27] persons. At least three Supreme Court cases have dealt with forfeiture proceedings triggered by s 295A.[28] In the *Rupawate*[29] decision for example, which dealt with a forfeiture order against James Laine and Oxford University Press, the publishers quickly apologised and withdrew the impugned book from publication despite the official ban being set aside. After incidents of public disorder occurred, a FIR was quickly issued in 2004. By the time the government's forfeiture order was appealed to the Supreme Court, it was already 2010.

These events can be contextualised from a perspective sensitive to India's legal history and culture. When India's Constitution was drafted in the aftermath of the Partition, the objective was to "establish a sense of security upon those who look upon each other with distrust and suspicion".[30] Freedom of the press[31] and faith were thus accommodated through articles 19 and 25 of the Constitution respectively, but reasonably abridged in the interests of security, morality, health and peace. Flowing from this constitutional architecture, the concept of 'group defamation' has found expression in the IPC as a means of identifying, criminalising and punishing forms of conduct and speech thought to be "inimical" to the public interest.[32]

Broadly, s 153A has been interpreted as a 'defamation of religion' provision.[33] It criminalises the promotion or attempt to promote hatred or ill-will between religious groups which is prejudicial to the maintenance of harmony and likely to disturb public tranquillity. Cases have interpreted the section to require that there be an intention to wilfully promote or attempt to promote hatred, inferred through the words used and extrinsic evidence.[34] Importantly though,

22 James Raven, 'Introduction: The Resonance of Loss' in James Raven (ed), *Lost Libraries: The Destruction of Great Book collections Since Antiquity* (Palgrave Macmillan, 2004) 1, 19.

23 Apar Gupta, 'Five Questions on Penguin Books Withdrawing, 'The Hindu's: An Alternative History' *Bar and Bench* (online). 13 February 2014 <http://barandbench.com/content/212/five-questions-penguin-books-withdrawing-%E2%80%9C-hindu%E2%80%99s-alternative-history%E2%80%9D#.U3RFToGSzy9>.

24 Personal Communication with Lawrence Liang, 12 May 2014.

25 A G Noorani, 'Penguin & the Parivar'*Frontline* (online) 4 April 2014 <http://www.frontline.in/social-issues/penguin-the-parivar/article5787832.ece>.

26 Personal Communication with Lawrence Liang, 12 May 2014.

27 *State of Maharashtra v Sangharaj Damodar Rupawate* (2010) 2 OJR 194.

28 *Harnam Das v State of UP* (1961) AIR 1662; *State of UP v Lalai Singh Yadav* (1997) AIR 202; *State of Maharashtra v Sangharaj Damodar Rupawate* (2010) 2 OJR 194.

29 *State of Maharashtra v Sangharaj Damodar Rupawate* (2010) 2 OJR 194.

30 Bharat Bhushan Gupta, *The Seven Freedoms* (Ashish Publishing, 1977) 3.

31 This extends to publishers: *W N Srinivasa Bhat v The State of Madras* (1951) IMLJ 115.

32 Thomas David Jones, *Human Rights: Group Defamation, Freedom of Expression and the Law of Nations* (Kluwer Law International, 1998) 88; *Beauharnais v Illinois* 343 US 250 (1951) 255-257 (Frankfurter J).

33 Abhinav Chandrachud, 'Speech, Structure and Behaviour on the Supreme Court of India' (2012) 25 *Columbia Journal of Asian Law* 222, 235.

34 *P K Chakravorty v Emperor* 1926 AIR (Cal) 113; *Satya Ranjan Bakshi v Emperor* 1929 AIR (Cal) 309; *Lajpat Raj v Emperor* 1928 AIR (Lah) 245; *Kali Charan Sharma* 1927 AIR (All) 654.

35 *Bilal Ahmed Kaloo v State of Andhra Pradesh* (1997) Crl A No 81/97.

to trigger the provision's operation there must be at least two groups involved.[35]

Section 295A serves a similar purpose by criminalising deliberate and malicious acts intended to outrage the religious feelings of any class by insulting their religion or religious beliefs. In the seminal ruling in *Ramji Lal Modi v The State of UP*[36] the Supreme Court confirmed its constitutional validity in terms of article 19 which guarantees freedom of speech subject to eight exceptions. Public order is one among them. However, the Chief Justice was at pains to point out that s 295A only penalises conduct that has been 'perpetrated with the deliberate and malicious intention of outraging...religious feelings'.[37] Proof of *mens rea* is required[38] and there is a high burden of proof.

On this analysis, it would have been difficult to argue Doniger's book contravened s 153A. There were no reports that the book had inspired ill-will between classes or religions. In spite of Doniger making it clear that 'I wanted to put into my book precisely those parts of history that they don't like',[39] the degree of malice demanded by s 295A is difficult to satisfy. One factor weighing against the publishers was an online petition that had amassed 11,000 signatures claiming there were 24 factual errors in the book.[40] However, procedural requirements also placed Penguin in a strong legal position. Nevertheless, it would have been difficult for Penguin to successfully argue its case without significant political ramifications. Sections 153A and 295A could not have been validly entertained by any court without the 'previous sanction'[41] of the government. Had the SBA sought consent, the matter would have escalated and entered directly into an electoral process primed for controversy.

On one view, branding the jurisprudence around these two provisions as doctrinally indeterminate is defensible when the law is viewed through a commercial eye which privileges certainty. The label is also possibly the result of a lack of substantial judicial consideration of these provisions: criminal prosecutions are rare.[42] Even with the possibility of legal victory, it appears the judicial disposition was set against Doniger. Batra alleged a judge hearing the case had said to him, 'I started to read it, but I stopped halfway because it was so vulgar and dirty.'[43] Pursuing legal vindication before this ostensible judicial mindset would have been fraught with risk.

A NO-COST SETTLEMENT?

'It's a shame that Penguin lost the lawsuit,' Doniger was later quoted as saying.[44] Even if the settlement was coloured as a moral loss for the author and publisher, it represented a partial commercial triumph. Penguin lawyers apparently knew "winning the case was impossible"[45] and informed Doniger that settlement would be delayed as long as possible to keep the book in print (and naturally produce sales).

Based on classic litigation strategy[46] and the meagre facts known to the public, settlement appeared viable. Litigation in India is unsurprisingly costly and as *Rupawate* showed, comically sluggish. Given the difficulty of distilling certain jurisprudence on the IPC provisions, the high likelihood of having to appeal to the Supreme Court would further extend the litigation cycle. Empirical research also shows that "speech cases are not a high priority" for the highest court in the land.[47] In a largely sensitive political context, this judicial canter generates uncertainty.

A private settlement avoided an official ban and arguably, best leveraged the division of rights between the parties

Aside from the content, the way Doniger framed her agenda in the book would have also presented a risk for the proceedings. Generating testimony and precedent on the question of intention would be unfavourable, particularly when coupled with the possibility of an official ban. If her detractors correctly cited factual errors in the book, the publishers would certainly be ill-disposed towards judicial findings of fact on the matter.

A private settlement avoided an official ban and arguably, best leveraged the division of rights between the parties. Doniger retained copyright in the publication with Penguin operating as publishers and distributors of the work in India. If Penguin withdrew in the absence of a government ban, Doniger would technically be able to publish through other

>

36 (1957) AIR 620.

37 (1957) AIR 620.

38 *Sujato Bhadra v State of West Bengal* (2005) 3 CALLT 436.

39 Tabb, above n 14.

40 Ibid.

41 *Code of Criminal Procedure 1973* s 196(1).

42 Jones, above n 32, 215.

43 Barry, above n 17.

44 Tabb, above n 14.

45 Ibid.

46 Jacob Horowitz, 'Why Going to Trial is a Bad Bet (But if you Must, How to Improve the Odds)' *Litigation Strategy Series* (Law Society of NSW, 2011); Larry Teply, *Legal Negotiation in a Nutshell* (Thomson West, 2nd ed 1992).

47 Chandrachud, above n 33, 222, 257.

Pulp Non-Fiction [CONT'D]

> entities or at a more favourable time. Reports emerged quickly at the time, that the New York arm of Penguin, unaffected by the terms of the settlement, was "considering sending 3,000 copies of the book to sell in India".[48] At least two other publishers allegedly offered to re-publish the now notorious tome.

This transaction raises deeply uncomfortable questions about cultural regulation by non-state actors

PROFITABLE PROVOCATION

"You'll be happy to hear about an interesting transaction I witnessed today," a scholar wrote to Doniger. "My friend walked into one of the larger bookstores and asked for a copy of your book. Within a minute the paperback edition of *The Hindus*...discreetly packed away in a paper bag, was produced from some back area of the store and handed over to her. So the book is still being sold right here. This is India."[49]

This story was relayed to Doniger less than a month after the pulping announcement.

The resonance of the forbidden and the pleasure of possessing illicit cultural artefacts lingered in the aftermath. William Mazzarella's classic words on the art of 'profitable provocation'[50] best captures these shifting lines between law, censorship, reputation and publicity:

As a gamble on publicity, cultural regulation is, for all its apparently routinised banality, an uncertain and open-ended venture.[51]

Lawsuits and complaints unlikely to succeed are strategically filed to stir public interest and pressure publishers – in turn, the notoriety delivers commercial windfalls. These provocateurs play cannily with the recursive relationship between the media and reputation[52] where private acts of cultural regulation become both centrally destructive and creative. Seemingly emboldened by the victory, the Aleph Book Company received demands from SBA seeking the withdrawal of Doniger's *On Hinduism*, published in 2013. In a public statement Aleph resolved not to reprint the book 'until an acceptable resolution' was found.[53] Its Chairman wryly noted that their stock had sold out "probably due to various statements made in public as well as the media coverage of your objections to the book published by Penguin".[54]

Aided by secrecy, a private settlement placed control over the media trial in the hands of Doniger and Penguin to manage its reputation where it mattered most: in public. Had the civil suit proceeded to final judgment, the scrutiny would have been greater, and more costly. This transaction raises deeply uncomfortable questions about cultural regulation by non-state actors. Where unaccountable private dealings determine the breadth and scope of state freedoms, publishers risk drawing the ire of the governed, and the governors. Provocation, then, becomes more political than profitable – a risk that settlement rarely handles, but which Penguin dangerously managed to gamble.

SHEENAL SINGH is a freelance writer and Graduate at MinterEllison.

48 Tabb, above n 14.

49 Ibid.

50 William Mazzarella and Raminder Kaur, 'Between Sedition and Seduction: Thinking Censorship in South Asia' in William Mazzarella and Raminder Kaur (eds), *Censorship in South Asia: Cultural Regulation from Sedition to Seduction* (Indiana University Press, 2009) 1, 21.

51 Ibid.

52 See: Fraser P Seitel and John Doorley, *Rethinking Reputation: How PR Triumphs Marketing and Advertising in the New Media World* (Palgrave Macmillan, 2012); David Rolph, *Reputation, Celebrity and Defamation Law* (Ashgate, 2008).

53 'Doniger's Book On Hinduism Put on Hold' *The Indian Express* (online), 11 March 2014 <http://indianexpress.com/article/india/india-others/donigers-book-on-hinduism-put-on-hold/>.

54 Aleph Book Company, *Official statement from Aleph/Rupa Regarding On Hinduism by Wendy Doniger* (online), 10 March 2014 <http://alephbookcompany.com/sites/default/files/press/Official%20Statement.pdf>.

SAVE THE DATE

CAMLA AGM AND END OF YEAR DRINKS

THURSDAY 19TH NOVEMBER

The 2015 Communications and Media Law Association Annual General Meeting and end of year drinks function will be held on:

THURSDAY 19th NOVEMBER

5:45 pm AGM

6:30 pm End of year drinks

Hosted by: Ashurst - Level 11, 5 Martin Place, Sydney

CAMLA members have been sent the CAMLA AGM notice and CAMLA Board nominee forms.

RSVP to camla@tpg.com.au or (02) 4294 8059 by Thursday 12th November. Please indicate whether you will be also attending the Annual General Meeting.

ELECTRONIC COMMUNICATIONS LAW BULLETIN

CAMLA is pleased to offer our members the Communications Law Bulletin in electronic format with effect from the first issue in 2015.

Please contact Cath Hill: camla@tpg.com.au or (02) 4294 8059 to indicate your delivery preference from the following options if you have not done so already:

☐ Email ☐ Hardcopy ☐ Both email & hardcopy

CONTRIBUTIONS & COMMENTS

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in electronic format and comments should be forwarded to the editors of the Communications Law Bulletin at editor@camla.org.au or to

Valeska Bloch or Victoria Wark

C/- Allens
Deutsche Bank Place
Corner Hunter & Philip Streets
SYDNEY NSW 2000

Tel: +612 9230 4000
Fax: +612 9230 5333

CAMLA contact details:

Email: camla@tpg.com.au
Phone: 02 42 948 059
Mail: PO Box 237,
KINGSFORD NSW 2032

About CAMLA

The Communications and Media Law Association Incorporated (CAMLA) brings together a wide range of people interested in law and policy relating to communications and the media. CAMLA includes lawyers, journalists, broadcasters, members of the telecommunications industry, politicians, publishers, academics and public servants. Issues of interest to CAMLA members include:

- defamation
- broadcasting
- copyright
- advertising
- information technology
- freedom of information
- contempt
- privacy
- censorship
- film law
- telecommunications
- the Internet & online services

In order to debate and discuss these issues CAMLA organises a range of seminars and lunches featuring speakers prominent in communications and media law policy.

Speakers have included Ministers, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers specialising in media and communications law, and overseas experts.

CAMLA provides a useful way to establish informal contacts with other people working in the business of communications and media. It is strongly independent, and includes people with diverse political and professional connections. To join CAMLA, or to subscribe to the Communications Law Bulletin, complete the form below and forward it to CAMLA.

Disclaimer

The Communications Law Bulletin is the journal of the Communications and Media Law Association which is an independent organisation which acts as a forum for debate and discussion and welcomes the widest range of views. The views expressed in the Communications Law Bulletin and at CAMLA functions are personal views of the respective authors or speakers. They are not intended to be relied upon as, or to take the place of, legal advice.

For further information:

Visit the CAMLA website at www.camla.org.au for information about CAMLA, CAMLA seminars and events, competitions and the Communications Law Bulletin.

To: The Secretary, camla@tpg.com.au or CAMLA, Box 237, KINGSFORD NSW 2032
Phone: 02 42 948 059

Name:

Address:

Telephone: **Fax:**

Email:

Principal areas of interest:

I hereby apply for the category of membership ticked below, which includes a Communications Law Bulletin subscription, and enclose a cheque in favour of CAMLA for the annual fee indicated:

☐ Ordinary membership $130.00 (includes GST)

☐ Corporate membership $525.00 (includes GST)
(include a list of names of individuals - maximum 5)

☐ Student membership $45.00 (includes GST)
(include undergraduate full time student card copy)

☐ Subscription without membership $150.00
(includes GST) (Library subscribers may obtain extra copies for $10.00 each + GST and handling)