Australian Government

Department of Communications

Cloud Computing Regulatory Stock Take

Report – Version 1

May 2014

Copyright notice

Attribution

Use of all or part of this report must include the following attribution:

Using the Commonwealth Coat of Arms

The terms of use for the Coat of Arms are available from the It's an Honour website (see www.itsanhonour.gov.au and click 'Commonwealth Coat of Arms').

Providing feedback on this report

The Department of Communications welcomes feedback on this report to improve its usefulness to stakeholders. To assist stakeholders in providing their feedback, discussion questions are included at the end of each chapter. A full list of discussion questions is also available at **Attachment E**.

Feedback can be provided in the following ways:

Email (preferred): cloud@communications.gov.au
Post: The Director

Cloud Computing and Privacy

Department of Communications

GPO Box 2154

Enquiries about this report may be directed to the email address specified above.

Privacy

The Department is committed to protecting your privacy. The Department has obligations under the *Privacy Act 1988* (the Privacy Act). In particular, the Privacy Act contains the Australian Privacy Principles (the APPs) which govern how the Department collects, uses and discloses personal and sensitive information, and how individuals can access and correct records containing their personal or sensitive information.

You may make a submission to the Department anonymously or by using a pseudonym. If you include any personal information and/or sensitive information in your submission, this information will be collected by the Department. By providing the Department with your personal information and/or sensitive information, you consent to the Department collecting, using and disclosing that information in accordance with this Collection Notice.

As part of considering your submission, the Department may use your personal and/or sensitive information for the purpose of developing policies in relation to the subject of this paper. Further, the Department may also disclose your personal information to the Minister, other government agencies and by placing your submission on the Department's website (see above).

The Department may also use the personal information collected for the purposes of maintaining a stakeholder contact list. Your personal information may be used to contact you for the purpose of consultation on developing policies in relation to the subject of this paper or related subjects.

If you do not consent to the Department's collection, use and disclosure of your personal information in accordance with this Collection Notice, please do not provide your personal information to the Department. If you have already provided your information to the Department, please notify us immediately (see contact details above).

The Department will use the personal information collected from you for the primary purpose it was collected. The Department may use or disclose this personal information for another purpose (i.e. secondary purposes) if:

- you reasonably expect the information to be used for the secondary purpose;
- it is required or authorised by law or a permitted general situation exist under the Privacy Act;
- you give the Department permission, or
- the Department reasonably believes the use or disclosure is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

See the Communications website for more information on the Department's APP Privacy Policy.

Table of Contents

Terminology

The **Australian Communications and Media Authority** or the **ACMA** is an independent statutory authority that regulates communications, including the regulation of telecommunications service providers (carriers, carriage service providers and content service providers).

The **Australian Competition and Consumer Commission** or the **ACCC** is an independent statutory authority that regulates Commonwealth competition and consumer protection laws.

The **Australian Law Reform Commission** or the **ALRC** is an independent statutory authority that reviews Commonwealth laws.

Cloud service provider or provider, for the purposes of this stock take, refers to a business that provides cloud services to customers.

Community cloud services are those that allow infrastructure to be shared between users with common interests or needs.

Consumer, for the purposes of this stock take, includes individual, small business and not-for-profit consumers of cloud services.

Co-tenant cloud service, for the purposes of this stock take, is one in which the infrastructure is shared between users with a common purpose. A **multi-tenant** cloud service is one in which the infrastructure is shared between multiple users from different organisations.

Data portability refers to the ability to move data stored on a cloud service out of the cloud or into another cloud service.

Hybrid cloud services combine a mixture of public, private or community cloud services.

Interoperability is the capacity for systems to interact with one another.

Market failure is an economic concept that refers to a market that does not allocate resources in the most economically efficient way, to maximise the production of goods and services.

The **Office of the Australian Information Commissioner** or the **OAIC** is Australia's national privacy and freedom of information regulator. The Commissioners of the OAIC have a range of investigation and enforcement powers under the *Privacy Act 1988* and compliance monitoring functions under the *Telecommunications Act 1997*.

Private cloud services are provided specifically for use by a particular organisation. The service may be owned and operated in-house or by a third party provider.

Public cloud services are provided over the internet, via shared infrastructure, with data and services hosted from different locations around the world.

Resilience refers to the capacity for a service or network to continue to perform in the event of a service disruption.

Vendor lock-in occurs where a customer has high switching costs. This can be due to a range of factors, such as, the cost of changing providers, data portability, interoperability or lack of transparency of contract terms.

Disclaimer

This document has been prepared for consultation purposes only and cannot be taken in any way as expressions of Commonwealth policy or as indicating a commitment to a particular course of action.

Please note that this document provides factual information only and is not a substitute for legal advice. Cloud service providers and their customers should seek independent legal advice on their specific obligations.

Executive Summary

Cloud computing is the consumption of information and communications technology (ICT) over the internet, as a service. Cloud computing can offer a range of substantial benefits to many different types of organisations, but can be especially transformative for small organisations (such as small businesses and not-for-profit organisations) because they may lack access to capital for ICT investment and may lack ICT expertise.

Despite the clear benefits that cloud computing can offer small businesses, adoption in Australia has been limited compared to other OECD countries. For example, the MYOB 2013 Business Monitor, a study of over 1,000 Australian small to medium businesses, found that only 16 per cent are using cloud computing.[1] This is despite the finding that those businesses that are using cloud services were 106 per cent more likely to see a rise in revenue in the last 12 months.[2] There is limited data on the use of cloud services in the not-for-profit sector.

Part of the reason for these findings may be that small businesses may not be aware that they are using a cloud service. This is supported by the finding that 35 per cent of small businesses are not adopting cloud services because they lack knowledge about these services.[3]

Like all ICT, the use of cloud computing is a question of taking advantage of the innovation and productivity benefits of new technology while managing potential risks. Given the benefits that the cloud can offer small businesses and not-for-profit organisations in particular, and the low level of take up or awareness by these groups, this stock take focuses on the issues that may affect individual, small business and not-for-profit consumers of public paid-for cloud services (collectively referred to as consumers throughout the document).

[1] MYOB, *Business Monitor*, myob.com.au/myob/news-1258090872838?articleId=1257830858409, March 2013.
[2] Ibid.
[3] Ibid.

Consumers, small businesses and not-for-profit organisations need sufficient information and adequate protections, including appropriate regulatory settings, to acquire cloud services with confidence. This was a conclusion of the National Cloud Computing Strategy, released in 2013.[4] A vibrant Australian cloud services market, in which there is strong competition, benefits consumers through increased choice, better quality services and lower prices.

Role of the Australian Government

This stock take discusses a range of existing Commonwealth regulation that applies to the Australian cloud services market. Given the international nature of many cloud computing services, it is important that readers recognise that the Australian Government has a limited role in assisting the cloud services market to function efficiently. Nonetheless, the government does still have an important role to play by:

- leading by example with best practice use of cloud services[5]
- ensuring there are appropriate regulatory settings in place that provide for efficient markets and harmonious communities, while minimising compliance costs and red tape[6]
- assisting industry to understand the regulatory obligations that apply[7]
- developing and providing information, in collaboration with the private sector, to empower consumers to make informed decisions about cloud computing and other productivity-enhancing technology.[8]

Much of the regulation outlined in this document supports the efficient functioning of the Australian Cloud services market, including providing important consumer protections. There is, however, a need to reflect on the extent to which existing laws may constrain competition and innovation in the Australian cloud services market. This is an area in which stakeholder feedback can provide valuable information to government.

It is government policy that regulation should not be the default option for policy makers and should only be imposed where it provides a net benefit to the

[4] Department of Communications, *National Cloud Computing Strategy*, www.communications.gov.au/digital_economy/cloud_computing, May 2013.
[5] Liberal Party of Australia, *The Coalition's Policy for e-Government and the Digital Economy*, www.liberal.org.au/latest-news/2013/09/02/coalition%E2%80%99s-plan-digital-economy-e-government, August 2013, p. 20.
[6] Liberal Party of Australia, *The Coalition's Policy to Boost Productivity and Reduce Regulation*, www.liberal.org.au/boosting-productivity-and-reducing-regulation, August 2013, p. 5.
[7] Ibid, p. 21.
[8] Liberal Party of Australia, *The Coalition's Policy for e-Government and the Digital Economy*, www.liberal.org.au/latest-news/2013/09/02/coalition%E2%80%99s-plan-digital-economy-e-government, August 2013, p. 22.

community.[9] For this reason, sector specific regulation should be recognised as the very last option to be considered by decision makers. As one stakeholder has observed, 'cloud computing is not a technological revolution that requires separate, cloud specific rules'. This is consistent with the Australian Government's deregulation agenda, discussed in Chapter 7.

Scope of this stock take

This stock take is a foundational document intended to provide guidance on the regulation that applies to cloud services. The stock take does not provide a comprehensive review of all the regulation that applies to cloud services, but instead highlights some key areas in Commonwealth legislation that may apply.

This stock take is intended to provide:

- a basis to commence a discussion with consumers, industry and representative groups about issues affecting the take up of cloud services and the Australian cloud services market more broadly
- confidence to consumers and certainty to industry about the existing regulatory measures in place
- a decision-making tool to government, for identifying and addressing potential issues in the cloud services market.

The Department has also prepared a range of fact sheets for small businesses using cloud services. Visit the Digital Business website for more information.

This stock take covers the following areas, which have been identified as issues that may impact on either the Australian cloud services market or the take up of cloud services among consumers:

Chapter 1: Competition and copyright

Chapter 2: Contractual arrangements and consumer protection

Chapter 3: Data protection and privacy

Chapter 4: Cybersecurity

Chapter 5: Government use of cloud computing

Chapter 6: Law enforcement access to data in the cloud

Chapter 7: Regulatory burden

Each chapter contains an overview of:

- the way in which the issue may impact on cloud services
- the existing regulatory arrangements that apply to that issue

[9] Department of Prime Minister and Cabinet, *The Australian Government Guide to Regulation*, www.cuttingredtape.gov.au, March 2014, p. 2.

- a discussion of the potential indicators that suggest further work may be needed to clarify obligations and some of the key issues that may arise in terms of addressing any issues.

The stock take is not intended to provide an exhaustive list of the issues that may impact on cloud computing. The issues considered are those that were identified through research and in discussion with stakeholders.

The relevance of each issue will vary depending on:

- the type of consumer (that is, individual, small business or not-for-profit)
- the type of provider and service
- the purpose for which the service is being used
- the industry in which the user operates
- the regulatory obligations that apply.

This stock take includes an awareness of issues outlined by a range of stakeholders. In particular, in determining the relevant issues the stock take has drawn on a number of key sources. The department acknowledges the contribution of industry in the development of this document, particuarlly in relation to the expertise provided by:

- the Australian Information Industry Association (AIIA)[10] and its members, which have generously provided its subject matter expertise to the development of this document.
- The National Standing Committee for Cloud Computing (NSCCC)[11] and its members for their ongoing contributions and subject matter expertise.
- Information Integrity Solutions for its substantial and comprehensive contributions to the examination of privacy issues throughout the document.
- The Australian Communications Consumer Action Network (ACCAN) released a position statement in 2012.[12] The statement sets out a range of issues that ACCAN considers need to be adequately addressed for consumers to take up cloud services, which include accessibility, interoperability, ownership, privacy, redress, simplicity, security and transparency.
- NextDC and the University of New South Wales developed a white paper

[10] The AIIA is the peak representative body and advocacy group for the ICT industry in Australia. The AIIA published an advocacy paper in October 2012, www.aiia.com.au/?page=CloudComputing

[11] The NSCCC a multi-stakeholder advisory committee, comprised of senior executives from federal and state government agencies, industry leaders, the research community and advocacy groups. Visit www.globalaccesspartners.org/joint-ventures/nsccc for more information.

[12] ACCAN, *Position Statement: What consumers need from cloud computing*, accan.org.au/index.php/broadband/broadband-policy-positions/514-position-statement-what-consumers-need-from-cloud-computing, December 2012.

entitled 'Data Sovereignty and the Cloud'. The document outlines a series of issues central to the protection of data in the cloud.[13]

- The Department of Finance has developed a series of cloud computing guides, including a 'Better Practice Guide' and the 'Negotiating the Cloud: Legal issues in cloud computing agreements' document. These documents highlight a range of legal issues for agencies transitioning to cloud services that may be relevant to other consumers of cloud services.[14]
- Research on common terms and conditions in cloud service contracts, undertaken by Mark Vincent and Katrina Crooks.[15]

A full list of the private sector and community organisations that contributyed to this document is at **Attachment F**.

Given many of the regulatory arrangements discussed in this paper are outside of the policy responsibilities of the Communications portfolio, the Department has consulted broadly with relevant government departments and regulators prior to the release of the stock take.

Further and background information is provided in the following attachments:

Attachment A: Market failure and economic efficiency

Attachment B: List of relevant Commonwealth legislation

Attachment C: List of relevant state and territory legislation

Attachment D: International regulation of cloud services

Attachment E: List of discussion questions

What is cloud computing?

While there is no universally agreed definition of cloud computing, the definition developed by the United States (US) based National Institute of Standards and Technology (NIST) in 2011 is widely considered to be authoritative:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[16]

There are five essential characteristics that differentiate cloud services from

---

[13] D Vaile, K Kalinich, P Fair and A Lawrence, *Data Sovereignty and the Cloud*, Cyberspace Law and Policy Centre, UNSW Faculty of Law, July 2013.
[14] Department of Finance, *Negotiating the Cloud: Legal issues in cloud computing agreements*, Better Practice Guide, Version 1.1, www.finance.gov.au/cloud/, February 2013.
[15] M Vincent and K Crooks, *Cloud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 17.
[16] The definition of cloud computing used here is taken from: P Mell and T Grance, United States Department of Commerce, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Special Publication 800-145, p. 2.

traditional ICT services:

- **Capacity on demand** – the service already exists and can be provisioned when needed, usually through self-service interfaces.
- **Device agnostic** – users can access cloud services over a network through a broad range of devices, accessed over a standardised platform (such as a web browser).
- **Resource pooling** – shared computing resources can provide significant economies of scale which help reduce costs and accelerate innovation.
- **Scalability**[17] – users can scale cloud services up or down quickly and cheaply.
- **Metering** – users can measure their consumption of cloud services quickly and easily, and adjust it accordingly.

The three most common service models are Infrastructure as a Service, Platform as a Service and Software as a Service. Table 1 provides examples of these different service models.

Infrastructure as a Service	Platform as a Service	Software as a Service
Data storage	Operating system	Email and Word Processing
Processing power	Web servers	Human Resource Management
Server virtualisation	Development platforms	Customer Relationship Management (CRM)

Table 1 - Examples of cloud services

There are four cloud deployment models: public, private, community and hybrid. Table 2 describes public and private deployment options, which are at either end of a continuum.

Most large organisations will consume a mix of different types of cloud services, referred to as 'hybrid cloud'. Community cloud is particularly relevant to the public sector, as it allows infrastructure to be shared by a range of organisations with common interests or needs. A community cloud may have components of public and private cloud.

Cloud service type	Description

[17] Capacity on demand is a connected, but distinct concept to 'scalability'. Scalability refers to the cost of increasing or decreasing a characteristic of the service. In contrast, the concept of capacity on demand allows users to unilaterally provision services automatically, without requiring human interaction with each service provider.

Public cloud services	A public cloud provides services to users over the internet. Infrastructure is shared, and data can be located in different locations across the globe. Some of the most well-known public cloud providers are Google, Amazon Web Services and Microsoft. Public cloud services offer the five essential characteristics of cloud computing: capacity on demand, device agnostic, resource pooling, scalability and metering. Public cloud services are used by ordinary consumers and an increasingly large number of organisations.
Private cloud services	A private cloud supplies ICT services to an organisation or restricted group of organisations over a dedicated network link. The private infrastructure can be located on site or managed through an external provider. While private cloud services are quite similar to traditional ICT, they can offer some of the benefits of public cloud services to a limited degree. Private cloud services can also have better latency than other options. Private cloud services are typically used by large organisations, including government agencies, banks and insurance companies, which are able to generate some efficiencies of scale.

Table 2 - Cloud deployment options

Due to the variety of services offered under the umbrella of cloud computing, it is not possible to outline a single concept of cloud computing. Even ICT specialists do not share a common definition of cloud computing[18]. This broad concept of cloud computing may make it difficult to identify all the issues and regulatory measures that may impact on the provision of cloud services.

[18] Microsoft and Fujitsu, *Cloud in Australia*, Vol. 2 Q. 2, 2012.

Chapter 1: Competition and copyright

Discussion of issues

This chapter discusses issues affecting competition in the Australian cloud services market, including vendor lock-in and geographic price discrimination. It also looks at copyright law, which has the capacity to enhance or impede innovation and access to information in the cloud services market. This chapter also provides an overview of the arrangements under the *Competition and Consumer Act 2010* (Competition and Consumer Act) and the *Copyright Act 1968* (Copyright Act) and how they may impact on cloud services.

Australia is well-placed to support a vibrant cloud sector, through the rollout of the National Broadband Network (NBN), the Government's trade agenda and regulatory settings that support growth, foster innovation and protect users. There is a need to continue to look at ways to strike a balance between initiatives that foster competition in the Australian cloud services market and mechanisms that provide adequate protection for consumers of cloud services.

Vendor lock-in

Lock-in occurs where a consumer is unable to easily switch between providers to take advantage of better pricing or new and improved service offerings. Issues that may affect the ability of a consumer to change providers include costs associated with moving, the ability of different systems to interact with one another (referred to as interoperability) to enable data to be easily moved from one service to another and transparency of information enabling consumers to compare services. Lock-in not only impacts consumers, but can affect competition in the cloud services market by making it particularly difficult for new entrants to attract existing cloud users to their services. This issue could be addressed through the development of international standards to set requirements around the interoperability of cloud services.

Geographic price discrimination

Geographic price discrimination occurs when a different price is charged for the same product in different locations. There is no current regulation of ICT pricing in Australia, with businesses free to determine the price of their products and services based on supply and demand.[19]

In May 2012, the House Standing Committee on Infrastructure and Communications commenced an inquiry into the issue of IT pricing including software, hardware,

[19] The Treasury, Submission to the House of Representatives Standing Committee on Infrastructure and Communications, Inquiry into IT Pricing, www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=ic/itpricing/subs.htm, August 2012, p. 1.

music, games and e-books. In the course of the Committee's inquiry, numerous references were made to cloud services, particularly cloud software as a service. A submission from the Australian Information Industry Association notes:

> We have been advised by some vendors that they are sensitive to consumer pricing concerns. In some instances this has resulted in them changing their go-to-market strategies, including offering cloud and subscription offerings aimed to achieve greater price parity between the US and Australian prices. It should be noted in this context that the Government policy position on cloud will potentially have a significant impact, i.e. if policy settings mean companies are limited in what cloud services they can offer (i.e. a requirement to host data onshore) then there is a real risk that businesses will miss out on the benefits of cloud, i.e. improved cost efficiency and effectiveness.[20]

The Committee handed down its final report on 29 July 2013. The report notes the role of cloud services in potentially reducing the cost of ICT services for consumers, but none of the ten recommendations specifically relate to cloud computing. The Government is considering its response to the Committee's report.

Copyright

Copyright is one area in which technological advancement may have progressed beyond the scope of existing law, potentially creating impractical regulatory arrangements for users and providers of cloud services.

In June 2012, terms of reference were provided to the Australian Law Reform Commission (ALRC) to conduct an inquiry into copyright and the digital economy.[21] The ALRC considered whether the exceptions and statutory licences are adequate and appropriate in the digital environment. In undertaking its inquiry, the ALRC considered a range of guiding principles for reform of copyright laws. One such principle was ensuring that copyright law is able to respond to new technologies, platforms, and services while providing certainty as to the existence of rights and permissible use of copyright materials. In its Issues Paper, released in August 2012, the ALRC requested views on whether Australian copyright law is impeding the development or delivery of cloud computing services, and whether existing exceptions should be amended, or new exceptions created, to account for new cloud computing services. A discussion paper was released in June 2013.

The inquiry's final report was tabled in Parliament on 13 February 2014 and contained 30 recommendations for reform.[22]

Overview of existing regulation

Competition law

---

[20] AIIA, Submission to the House of Representatives Standing Committee on Infrastructure and Communications, Inquiry into IT Pricing, www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=ic/itpricing/subs.htm, July 2012, p. 10.

[21] ALRC, Copyright and the digital economy, www.alrc.gov.au/inquiries/copyright/terms-reference, June 2012.

[22] ALRC, Copyright and the digital economy, report 122, www.alrc.gov.au/publications/copyright-report-122, 13 February 2014.

The Competition and Consumer Act promotes competition and provides consumer protections through the regulation of certain anti-competitive behaviour.

Part IV of the Competition and Consumer Act covers a range of anti-competitive conduct, including:

- Cartel conduct – this involves the making of or giving effect to an agreement with a cartel provision that includes conduct such as price fixing, output restrictions, market sharing or bid rigging.
- Collective boycotts and anti-competitive agreements – collective boycotts involve agreements between two or more competitors to restrict the supply or acquisition of goods or services to or from a third party. Anti-competitive agreements are any agreements that have the purpose, effect or likely effect of substantially decreasing competition in a market.
- Misuse of market power – this includes conduct by a market participant with substantial market power that seeks to abuse the power to eliminate or substantially damage a competitor, prevent a person from entering a market or deter a person from competing in a market. It includes supplying goods or services at a price less than the cost of supplying those goods or services for one of the above purposes.
- Exclusive dealing – this includes supplying or acquiring goods and services under an agreement that restricts the ability to deal with others. This conduct is illegal where it has the effect or likely effect of substantially lessening the competition.
- Third line forcing – this involves exclusive dealing for products or services on the condition the buyer will acquire products or services from a third party. The practice is prohibited unless between related entities.
- Resale price maintenance – this is the setting of a price at which a reseller must supply products or services.
- Mergers and acquisitions – a merger or acquisition is prohibited where the effect would be to substantially lessen the competition in a market.

In addition, Part XIB of the Competition and Consumer Act regulates competition in the telecommunications sector with a focus on anti-competitive behaviour. Part XIB regulates the conduct of both carriers and carriage service providers in Australia. Part XIC of the Competition and Consumer Act promotes competition by ensuring access to essential telecommunications services is available to access seekers on agreed terms of declared services.

The Australian Competition and Consumer Commission (ACCC) has regulatory oversight of competition in Australia, including economic regulation of the communications industry. Key functions include promoting competition, remedying market failure, ensuring access to essential infrastructure and providing consumer protections.

Australian competition laws are designed to provide a competitive and effective

marketplace within Australia. Cloud service providers need to be aware of the regulations relating to restrictive practices.

On 4 December 2013 the Prime Minister, the Hon Tony Abbott MP, announced the Government would undertake a comprehensive review of competition laws and policy.[23] On 27 March 2014 the Government announced the terms of reference and review panel for the review.[24] It is anticipated that the review will be completed within 12 months.

Copyright law

Australian copyright law provides a person who creates copyright material with exclusive legal rights including the right to copy, publish, communicate and publicly perform the material. The Copyright Act seeks to balance the rights of the legitimate owners of copyright with the public interest in making copyrighted materials available by establishing a framework for the legal protection of ideas and information produced in certain forms. Copyright covers works produced in literary, dramatic, musical or artistic form as well as audio-visual items including sound recordings, films and broadcasts. The Copyright Act also contains exceptions under which certain dealing is exempt from infringement or can be authorised by the copyright holder.

General exceptions to copyright infringement include fair dealing, format and time shifting. The fair dealing exceptions set out specific purposes and the circumstances under which copyright may not be infringed, such as research or study. Under the exception for format-shifting, an individual may make a copy of a sound recording but may only use it on a device owned by the individual.[25] The time-shifting exception allows a person to copy television and radio broadcasts for private and domestic use for the purpose of watching them at a more convenient time. An exception also applies to temporary reproduction, including where the reproduction is for technical purposes only.[26]

New ways to access, use and storage of copyright material using digital technologies create grey areas in the law and, as a result, consumers and cloud service providers may inadvertently infringe copyright. Where a cloud service is used to distribute or store infringing copyright material, copyright issues may arise for both the cloud service provider and the user.

The extent to which the exceptions under the Copyright Act may apply to cloud

---

[23] The Hon T Abbott MP (Prime Minister), *Review of Competition Policy*, media release, Parliament House, Canberra, www.pm.gov.au/media/2013-12-04/review-competition-policy, 4 December 2013.
[24] Visit competitionpolicyreview.gov.au/ for more information.
[25] A similar exception applies to the copying of books, newspapers and periodicals but only enables one copy of each.
[26] Under sections 43A and 111A, a temporary reproduction of a work, an adaptation of a work or an audio-visual item is allowed where it occurs as part of the 'technical process of making or receiving a communication'. Section 47C provides an exception for the making of back-up copies of computer programs and 'any work or other subject matter held together with the program on the same computer system'.

services is unclear and will depend on the specific facts of the case, including the manner in which the cloud service is configured and used. The time-shifting exception may not apply to copyright material that is copied and stored onto a remote server. Likewise, the format-shifting exception may not apply where an individual seeks to play a copied sound recording on software stored in the cloud, rather than the user's own device. The exception for the making of back-up copies will also be relevant to cloud services as cloud service contracts generally set out the requirements for ensuring adequate back up of data stored in the cloud. The ALRC has noted that it is unclear whether the current law enables back-ups of copyright material to be copied and downloaded from remote cloud servers.

The Copyright Act also establishes a voluntary 'safe harbour scheme', creating legal incentives for carriage service providers to co-operate with copyright owners in preventing copyright infringement. The safe harbour scheme limits the remedies available against a carriage service provider for infringements that occur in the course of carrying out certain online activities, where the carriage service provider has satisfied the prescribed conditions.

Recent cases, including *National Rugby League Investments Pty Ltd v SingTel Optus Pty Ltd*[27], demonstrate that there is potential for a cloud service to infringe copyright. In that case, Optus subscribers were provided the TV Now service to record free-to-air television broadcasts and store them in the cloud to be replayed within 30 days on a web browser. The action was commenced by the owners of copyright in television broadcasts of sporting events, National Rugby League and Australian Football League (AFL), and Telstra, owner of an exclusive licence to broadcast the AFL over the internet. Two key issues were under consideration: whether it was Optus or the user of the TV Now service who was the 'maker' of the copy, and whether the time shifting exception in section 111 applied. On appeal, the Full Federal Court found that Optus could not rely on the time shifting exception as Optus was making the copy for commercial purposes, not for 'private and domestic' purposes. On this basis, Optus was found to have infringed copyright and ordered to pay costs.

Submissions to the ALRC inquiry have raised concerns with the existing exceptions, particularly in light of the Optus TV Now case, potentially inhibiting innovation in the growth and delivery of services that allow improved ways of consumers accessing copyright material.[28]

Some submissions showed support for a fair use exception to specifically address caching and indexing functions. For example, Optus noted that much of the traffic in data centres involves copying and backing up data, which may currently amount to an infringement of copyright law.[29] The Law Council of Australia indicated that the existing treatment of caching under copyright law has resulted in 'several

[27] [2012] FCAFC 59.
[28] ALRC, Copyright and the digital economy, discussion paper 79, www.alrc.gov.au/publications/copyright-and-digital-economy-dp-79, 5 June 2013, p.102.
[29] Ibid, p. 159.

overlapping, but distinct provisions aimed at the same basic phenomenon and offering only partial and uncertain protection'.[30]

In its Final Report on Copyright and the Digital Economy, the ALRC has recommended that a new fair use exception be introduced under which certain uses do not infringe copyright.[31] Under the proposed exception there would be a non-exhaustive list of four factors for consideration in determining whether a use can be considered fair under the Copyright Act. These include:

- the purpose or character of the use
- the nature of the material used
- the amount or substantiality of the use
- the effect of the use on the potential market value.

The Government is now considering the recommendations made in the Final Report.

Potential triggers

In its Broken Concepts 2013 Report, the Australian Communications and Media Authority (ACMA) identified a range of concepts within the telecommunications industry which it considers to be 'broken' within the context of new and emerging technologies, service models and market structures.[32] Portability (or vendor lock-in) is an area in which the traditional concept, which was primarily relevant to the ability of a customer to 'port' their mobile or fixed line number from one service provider or geographic location to another, may now be expected by consumers to apply more broadly to the storage of content on a range of devices and platforms. The issues of portability and interoperability are particularly relevant in the cloud environment where there is the capacity for a customer to be negatively impacted by the inability to effectively transition their data from one service to another, as well as for it to impact on competition more broadly. The ACMA notes that the concept of portability may need to be extended to provide consumers with enhanced control over access to their data.[33] It is noted that the European Union (EU) is considering amendments to its Data Protection Directive[34] to provide consumers with the right to portability of their data (see **Attachment D** for more information).

Triggers that may be indicative of a lack of effective competition in the cloud services

[30] Ibid.
[31] ALRC, Copyright and the digital economy, report 122, www.alrc.gov.au/publications/copyright-report-122, Chapter 5, 13 February 2014.
[32] ACMA, *Broken Concepts – A 2013 update on the Australian communications legislative landscape*, www.acma.gov.au/theACMA/About/The-ACMA-story/Connected-regulation/broken-concepts, June 2013, p. 88.
[33] Ibid, p. 89.
[34] The full name of the directive is the European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

market may include:

- **Barriers to entry:** New entrants may experience difficulty in entering the market. This could be measured through the number of complaints by new or potential new entrants to the ACCC or by measuring market share.
- **Vendor lock-in:** Cloud service customers could have difficulty changing providers. The number of complaints by cloud service customers to the ACCC (or other regulatory bodies, such as the Telecommunications Industry Ombudsman or the ACMA) may indicate a lack of competition and consumer choice.
- **Regulation is limiting innovation due to out-dated concepts:** Cloud service providers may raise concerns about the application of existing regulatory frameworks to new technologies. Feedback from industry and industry groups through consultation processes, such as the ALRC's copyright review, can be useful in identifying the impact of regulation on the cloud services market. Legal disputes, such as the Optus TV Now case, may indicate that there is a need to reconsider the application of laws in light of new delivery models.
- **Significant price differentials and difference of service offerings between jurisdictions**: Higher prices and less choice for cloud products could be an indicator that the price of doing business in Australia is higher than in other jurisdictions. Further, significant differences in the terms and conditions for service offerings between jurisdictions may be indicative of broader problems in the Australian market. Over-regulation could be a contributing factor, although there are likely to be other factors (such as exchange rate differences) that offer better explanations.

Conclusion

Strong competition in the cloud services market encourages greater service innovation and enhances the services available to consumers. A robust competition framework is underpinned by regulatory certainty in areas impacting on competition and innovation, such as copyright law.

Chapter 1 Questions

1. Are there other issues that impact on competition in the Australian cloud services market? How does the cost and complexity of Australian regulation compare to other jurisdictions?
2. Is there evidence of anti-competitive practices in the Australian cloud services market? If so, how could these issues best be addressed?
3. Are existing copyright laws impacting on the Australian cloud services market? How could any issues best be addressed?
4. What indicators should government consider to determine whether there are issues affecting the competitiveness of the Australian cloud services market?

Chapter 2: Contractual arrangements and consumer protection

Discussion of issues

This chapter discusses contractual arrangements and consumer protection issues in the Australian cloud services market, including transparency, unequal bargaining power, service availability, transitional arrangements, customer support and complaints mechanism and enforcement issues. This chapter also provides an overview of consumer protections under the Australian Consumer Law, the *Telecommunications Act 1997* and the *Broadcasting Services Act 1992*.

The reality of many ICT service arrangements is that small business, individual and not-for-profit consumers may have little capacity to negotiate the terms of the contract and may rely on standard form agreements. The inequality of bargaining power may raise significant issues around the capacity for the contract to meet the specific needs of the customer, including any relevant regulatory obligations.

Where the service no longer meets the needs of the customer, whether through changes to the service itself or simply changes to the customer's requirements, they will need to weigh up whether moving to another service is the best option, given there may be cost and technical problems with moving to another provider. The ability to change providers where a service no longer meets the customer's needs is particularly important.

Transparency

Simplicity and understanding of important terms may play a key role in encouraging take up of cloud services among small businesses and not-for-profits that may not have ready access to legal or ICT expertise, to provide advice on complex terms and conditions. Not only is transparency important for consumers to understand how their service will be delivered, but also in enabling consumers to readily compare the key terms and conditions of various cloud service providers prior to choosing a service or when changing providers.

Consumers should understand the pricing model used by a cloud service provider before entering into an agreement, including charges that may apply to changes in use of the service, such as scalability, early termination of the contract, access to data when the contract ends, and value-add services. For example, some providers may charge more to scale the service where the customer's website experiences a sudden and unanticipated increase in traffic. There may also be costs associated with the provision of additional services to meet the customer's needs, such as making special arrangements for the storage of confidential or personal information.

As larger organisations or even governments negotiate more favourable terms, these are likely to filter through to other consumers of cloud services, making standard

terms more user-friendly.[35]

Unequal bargaining power

It may not be possible as a consumer to negotiate a change to the standard terms and conditions for a cloud service. Even where there is scope for the customer to negotiate some terms of the contract, this may be undermined by the ability of the cloud service provider to unilaterally alter the terms of the agreement.[36]

Research on contractual terms in cloud service contracts found that most contracts require the provider to give notice of changes to the terms and conditions for providing the service, although not necessarily directly to the customer.[37] However, some contracts allowed the provider to alter the terms and conditions without notifying users of the service. In other cases, the cloud service provider has sought to assure customers that it will not change the terms of service, except where it is expressly agreed between the parties.

Service availability

The level of service availability will generally depend on the plan selected. Service level agreements usually set out terms such as the targets for service availability and exclusions that may apply. Often outages that occur as a result of *force majeure* (where an extraordinary event outside of the control of the parties occurs), scheduled maintenance, misuse by the customer, or an outage elsewhere in the internet, will be excluded for the purposes of measuring service availability.[38] In some cases the cloud service provider may offer service credits where the service availability falls short of the service level agreed.[39]

Consumers should pay attention to the service availability arrangements set out in the contract or any additional documents, such as service level agreements or service provider policies that may affect the provision of their service. Research on terms in cloud service contracts found some of the service credit regimes contained so many caveats as to render them practically useless.[40] Service availability that falls short of the agreed service levels or the marketing or contractual representations made by the cloud services provider may give rise to rights under consumer protection legislation.[41]

---

[35] W Kuan Hon, C Millard and I Walden, 'Negotiating the cloud: Looking at clouds from both sides now', *Stanford Technology Law Review*, Vol. 16, No. 1, Fall 2012, p. 84.
[36] M Vincent and K Crooks, *Cloud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 17.
[37] Ibid.
[38] Ibid.
[39] Ibid.
[40] Ibid, p. 13.
[41] Ibid, p. 12.

Transitional arrangements

What is interoperability?

Interoperability is the ability of systems to work together. It affects a range of areas in cloud services, including the ability to transition existing resources into the cloud without changing the format, the ease of interaction between applications, for example, where the customer uses multiple services and the ease of migrating data from the cloud, whether to another provider or deployment model.

The ability to transition data or services to another provider or simply out of the cloud with minimal inconvenience and cost is a key issue. Many contracts do not adequately provide for transitioning out of the service, as there is limited post-termination assistance offered and many contracts provide for the immediate deletion of the data stored on the service (that is, without a period during which to transition data to another service or storage arrangement).[42] Interestingly, research indicates that some contracts do not have a specific obligation to delete data at the termination of the contract, including personal information.[43] This may be inconsistent with specific obligations under the *Privacy Act 1988* to delete personal information once it is no longer needed.

Ideally, the contract should specify the arrangements upon termination for return of data, in an accessible non-proprietary format that is readily useable by the customer, and deletion of any backed-up versions of data.

There has been some movement recently to the use of open source applications to provide cloud services. The ACMA has noted the importance of portability and interoperability in enabling consumers to access cloud services, promoting competition and removing barriers that prevent end users from moving between services and providers.[44]

Customer support and complaints mechanism

An effective complaint-handling mechanism is important in ensuring consumer confidence in the use of cloud services and enabling consumers to seek support and redress when something goes wrong. While some consumers may be satisfied with simply discontinuing their use of a service if it does not meet their needs, others may prefer to enforce their rights, either directly with the provider or through the relevant regulatory body.

In the case of cloud services, effective complaint mechanisms may be more important as the service is offered over the internet without the same physical presence of more traditional services and, in some cases, with the service provider located in another jurisdiction. Also, customers moving to a cloud service for the first

[42] M Vincent and K Crooks, *Cloud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 15.
[43] Ibid, p. 16.
[44] ACMA, *The Cloud – services, computing and digital data*, Occasional Paper 3, www.acma.gov.au/Citizen/Stay-protected/My-online-world/Staying-safe-online/coherent-regulation-best-for-cloud-services, June 2013, p. 15.

time may require additional support with their transition, making the support and complaints mechanism more important in the overall customer experience.

In addition to the complaints mechanism (if any) in the contract, the cloud service provider may seek to apply the laws of the jurisdiction in which it is based where a dispute arises (referred to as choice of law). This may mean that the customer may need to initiate action in a foreign jurisdiction. In many cases terms and conditions indicate that the applicable law is that of the country in which the provider is based.[45] This may have practical implications as the customer may be effectively denied the opportunity to seek redress for a contractual dispute.

Enforcement issues

In the event that a customer cannot resolve their complaint directly with the service provider, they may need to refer the issue to the relevant regulator. It is important that customers are aware that they may have a range of rights and that, even where a contract seeks to impose different rights and obligations or even expressly exclude statutory rights and obligations, they may have no effect for a consumer covered by Australian law. For example, the Competition and Consumer Act provides non-excludable guarantees that apply to Australian consumers and cannot be excluded through the terms of a contract.

The largely untested nature of many aspects of cloud services may impact the enforcement of laws in this area. Due to the often complex contracting arrangements associated with cloud services, it may not be clear whether non-Australian cloud service providers are subject to Australian law. Further, where a cloud service provider is located outside of Australia it may be impractical to take enforcement action against them. Ultimately the jurisdiction in which a claim can be brought will depend on the specific circumstances of the case, such as the location of the parties to the contract, the location of equipment and the terms agreed to in the contract.

Overview of existing regulation

In Australia, general consumer rights are set out in the Australian Consumer Law (ACL), contained in Schedule 2 to the *Competition and Consumer Act 2010*. The ACL is a national application law, which means it is enacted in legislation in each state and territory to provide for consistent application of consumer rights across Australia. As a law of the Commonwealth, the ACL applies to the conduct of corporations, meaning a trading or financial corporation formed within Australia or incorporated within a territory of Australia, or a foreign corporation, or a holding company of one of these.[46] As an application law of states and territories, it applies to both corporations and individuals. Foreign companies carrying on business in Australia will generally be caught by the provisions in the Competition and Consumer

[45] M Vincent and K Crooks, *Cloud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 4.
[46] Sections 4 and 131(1), *Competition and Consumer Act 2010.*

Act. However, as noted above, there may be practical impediments to enforcing the ACL against a service provider based outside Australia.

The ACL commenced on 1 January 2011, introducing enhanced redress mechanisms and enforcement powers for the ACCC and a new unfair contract terms regime. The ACL varies in its application, depending on the practice, as set out below.

Unfair contract terms

Under the ACL a term in a standard form contract is void where the term is unfair.[47] There is an automatic presumption that a contract is standard form where it is alleged by one party to the proceedings[48] and there are a range of factors that may be considered by the court.[49] The ACL indicates that a contract may be standard form where it was prepared by one party prior to discussion with the other, where one party has more bargaining power than the other, where the terms and conditions were on a 'take it or leave it' basis, whether there was opportunity to negotiate the terms and whether the terms take account of the specific characteristics of the parties or transaction.

A term is unfair when it causes a significant imbalance in the rights and obligations arising under the contract, is not reasonably necessary to protect the legitimate interests of the supplier and would cause financial or non-financial detriment to a party. The ACL sets out a range of examples of terms that may be considered unfair, including terms that provide one party but not the other with powers such as the ability to avoid or limit performance, terminate the contract, vary the terms of the contract, renew or not renew the contract, vary the characteristics of the goods or services to be supplied, or assign the contract to the detriment of another party without that other party's consent.[50] Unfair contract protections apply only to standard form contracts for goods and services actually acquired for personal, domestic or household use or consumption. As such, small businesses and not-for-profit organisations are not currently protected. However, the Australian Government and state and territory governments are considering extending the unfair contracts regime to small business. A comprehensive consultation process is expected to commence in the coming months.[51]

The ICT sector tends to use standard form contracts that favour the provider of the goods and service. While some larger business customers may have the capacity to negotiate contract terms, the majority of contracts for consumers are likely to be standard form, making the unfair contracts regime under the ACL particularly relevant. Based on the examples provided by the ACL, a term may be unfair where the cloud service provider has certain powers that are not afforded to the customer, such as varying the characteristics of the cloud service, including the speed, size or

[47] Section 23, Schedule 2, Competition and Consumer Act.
[48] Subsection 27(1), Schedule 2, Competition and Consumer Act.
[49] Subsection 27(2), Schedule 2, Competition and Consumer Act.
[50] Subsection 25(1), Schedule 2, Competition and Consumer Act.
[51] Visit www.consumerlaw.gov.au/content/Content.aspx?doc=caf/meetings/005.htm for more information about the unfair contracts regime.

security settings, without the customer's agreement.

False or misleading representations and unconscionable conduct

The ACL also prohibits the making of a false or misleading representation about goods or services, including:

- that the service meets particular standards or quality, value or grade
- that the service has been acquired by a particular person
- that the service has sponsorship, approval, performance characteristics, accessories, uses or benefits, or
- in regards to price.[52]

The protections against misleading representations apply to all businesses and individuals.

False or misleading representations may arise where a cloud service provider indicates, either in the contract or, through marketing material or policy documents, certain aspects of the service which are found to be false or misleading. Examples in the area of cloud services may include the service availability or that the service meets certain security standards.

In addition, the Act prohibits unconscionable conduct in connection with the supply of goods and services. The court can consider a range of factors in determining whether conduct is unconscionable, including the relative strengths of the bargaining positions of the parties; whether the customer was required to comply with terms not reasonably necessary to protect the legitimate interests of the supplier; whether the customer was able to understand documents relating to the supply of the goods or services, any undue pressure or influence or unfair tactics used against the customer or the customer's agent; the amount and circumstances under which the customer could have obtained identical or equivalent goods or services; the terms and conditions of the contract, including whether they were negotiated between the parties; the conduct of the supplier in complying with the contracted terms and conditions; and the extent to which the parties acted in good faith.[53] Unconscionable conduct protections apply to all businesses and individuals.

Consumer guarantees

Consumer guarantees are also included in the legislation, including that the services are provided with due care and skill and are fit for a particular purpose if such a purpose was implied or expressly made known to the provider. Such warranties give consumers the right to seek a refund or replacement of goods or services. The consumer guarantees regime applies to purchases under $40,000 or, where they exceed the amount, the services 'were of a kind ordinarily acquired for personal,

[52] Subsection 29(1), Schedule 2, Competition and Consumer Act.
[53] Subsection 22(1), Schedule 2, Competition and Consumer Act.

domestic or household use or consumption'.[54]

Consumer guarantees may also be applicable where a service purports to do something and fails to, for example, where service availability or quality fails to meet the standards specified by the provider (whether in the contract, marketing material or policy documents).

It is important to note that the protections provided by consumer law cannot be excluded by contract. For example, the contract cannot exclude the operation of consumer guarantees.

In general terms:

Carriage Service Providers are businesses that supply telecommunications services (which includes internet services) to the public. Section 87 of the Telecommunications Act defines carriage service provider.

Carriers are licensed owners or operators of communications infrastructure that is used to supply telecommunications services to the public. Many carriers are also carriage service providers.

Telecommunications and broadcasting regulation

The two principal classes of entities regulated by the *Telecommunications Act 1997* (Telecommunications Act) are carriers and carriage service providers. The owner of a network unit (fixed line or radiocommunications facility) used to supply carriage services to the public must hold a carrier licence (except in limited circumstances) and is known as a carrier.[55] Carriage service providers supply listed carriage services (services for carrying communications by means of guided and/or unguided electromagnetic energy between two or more points, one of which must be located in Australia) to the public using network units owned by one or more carriers.

Under section 44 of the Telecommunications Act, a carriage service is supplied to the public where it is used for[56]:

- the carriage of communications between two end users where neither is in the 'immediate circle' of the supplier of the service (for example, the service provider and its employees), or
- the carriage of 'point-to-multipoint services' to end users (this is effectively communication with more than one end user simultaneously) where at least one end user is outside the immediate circle of the supplier.

While cloud service providers are not necessarily covered by the Telecommunications Act, there may be circumstances in which the nature of services provided means that a cloud service provider will be a carriage service provider and subject to the obligations in the Telecommunications Act. Given the elements in the definition of a carriage service provider, whether a cloud service provider is captured

[54] Subsection 4B(1)(b), Competition and Consumer Act.
[55] Part 3 of the Telecommunications Act.
[56] Section 44 of the Telecommunications Act.

by the definition will depend on the specific products or services provided. For example, a system provided by a cloud service provider that allows data to be uploaded and stored on its service may not be considered to be a carriage service, whereas a webmail service that enables users to communicate with other end users, may be considered a carriage service. Accordingly, a cloud service provider supplying multiple products may be considered a carriage service provider for the purposes of some services and not for others.

Carriage service providers and, in some cases, content service providers must comply with the service provider rules set out in Schedule 2 of the Telecommunications Act. Many of these rules are specific to the provision of fixed line or mobile services and would not be relevant in the cloud context even if providers were deemed to be covered by telecommunications regulation.

However, one area of relevance is the ability to take complaints to an industry ombudsman. Under the *Telecommunications (Consumer Protection and Service Standards) Act 1999*, carriers and eligible carriage service providers are required to join the Telecommunications Industry Ombudsman (TIO) scheme, which is an independent body that provides a dispute resolution service to small businesses and consumers. Complaints about telecommunications services must first be referred to the relevant carrier or eligible carriage service provider for the opportunity to address the concerns, prior to being raised with the TIO. The TIO can investigate complaints relating to the supply of a landline service to residential or small business customers, a mobile telecommunications service or an internet, as well as some related matters. The TIO has authority to make binding decisions up to the value of $50,000 and recommendations up to the value of $100,000. It is funded through industry fees.

In circumstances where a cloud service provider is a carriage service provider within the meaning of the Telecommunications Act it may also be required to comply with elements of the Telecommunications Consumer Protection Code (TCP). The TCP Code deals with privacy, advertising, point of sale information, billing, credit management, customer transfer and complaint handling.

The concept of a carriage service provider is also relevant to other regulation, including the *Telecommunications (Interception Access) Act 1979* and the safe harbour provisions under the *Copyright Act 1968*.

The Telecommunications Act also establishes a third type of entity, a content service provider, which supplies content services to the public, such as a pay TV service, using a listed carriage service. A content service provider uses a 'listed carriage service' to supply a content service to the public.[57] A content service is broadly defined to include 'any online service', specifically to allow it to capture emerging services, and is likely to include a cloud service. For the purposes of supplying a content service to the public there must be 'at least one end-user of the content

[57] Section 97 of the Telecommunications Act.

service [who] is outside the immediate circle of the supplier of the content service'.[58]

The *Broadcasting Services Act 1992* regulates the types of content that can be hosted over the internet. Schedules 5 and 7 set out the rules governing the broadcasting of online content by internet service providers and content service providers in Australia. Internet content hosts are also captured by the Act where they host or propose to host internet content in Australia. The ACMA administers a co-regulatory scheme under which prohibited content or potentially prohibited content cannot be hosted within Australia. The ACMA also administers the Online Content Scheme for dealing with illegal online content. This includes a process for notifying state or territory law enforcement agencies, the Australian Federal Police or international bodies where content is potentially illegal.

Potential triggers

The ACMA's Broken Concepts Report identified a number of core concepts that underpin the regulation of telecommunications services that the ACMA considers to be 'broken', including the licensing of carriers and concepts of 'carrier', 'carriage service provider' and 'network unit'. In particular, it was noted that the emergence of technologies such as cloud has blurred the line between infrastructure and service providers. The ACMA considers that many of the existing key concepts do not adequately capture new services, such as those that are provided 'over the top' of a traditional carriage service and do not involve a network unit even if they are 'supplied to the public'.[59]

The ACMA also noted that the expansion in the content services market of cloud and application-based services changes the relevance of internet service providers as the main entity regulated in this area.[60]

Some potential triggers that may indicate that consumer protection is inadequate in its application to cloud services may include:

- **Lack of understanding among industry:** Cloud service providers may indicate that telecommunications and broadcasting legislation is unclear in its application to cloud services. A lack of clarity increases risk and compliance cost. Problems in this area could be measured though industry representations to government, such as through government reviews. It could also be measured through engagement between regulators, such as the ACMA, and cloud service providers.
- **Significant consumer and contractual issues:** If cloud service providers did not take adequate steps to comply with consumer law, further work may be needed to ensure cloud service providers understand and comply with their

[58] Ibid.
[59] ACMA, *Broken Concepts – A 2013 update on the Australian communications legislative landscape*, www.acma.gov.au/theACMA/About/The-ACMA-story/Connected-regulation/broken-concepts, June 2013.
[60] Ibid, p. 81.

obligations. This may be identified through complaints to the ACCC, ACMA or other relevant regulatory bodies (such as state or territory fair trading associations). It could also be measured by considering whether the standard form contracts developed by cloud service providers are consistent with Australian law.

- **Difficulties in understanding or enforcing contracts:** If consumers experience problems understanding or enforcing cloud service contracts, further work may be needed to enhance consumer redress mechanisms. This could be measured through:

  - The number of complaints about contractual or other consumer protection issues made to the ACCC or the ACMA, such as misleading and deceptive conduct, unfair contract terms or even 'bill shock', may indicate that the industry generally was subject to information asymmetry (this concept is discussed in Attachment A. Also, the extent to which complaints are made to the incorrect regulatory body may indicate that consumers do not have sufficient information about how to initiate a complaint about their cloud service.
  - Research on key contractual terms as they evolve over time may also assist in identifying the extent to which key concerns are being addressed by industry in a responsive way.
  - Ongoing consumer surveys, such as the annual Australian Consumer Survey, may provide insight into the degree to which consumers are able to understand contractual terms and adequately address issues that arise during the term of the contract. It may indicate areas where additional education could be targeted to particular consumers, either by government or by industry.

Conclusion

Adequate consumer protection is an important aspect of ensuring consumer confidence in the use of cloud services. This is particularly so for individual, small business and not-for-profit consumers who may not have the same capacity as larger businesses to negotiate terms and conditions that meet their specific needs. Both consumers and industry need to be aware of their rights and obligations, as well as how to make a complaint in the event that something goes wrong.

Chapter 2 Questions

5. Are there other contractual or consumer issues affecting consumers of cloud services? How could any issues best be addressed?
6. Is the current coverage of consumer, telecommunications and broadcasting law appropriate? What opportunities exist to provide greater clarity for industry and better protection for consumers?
7. Do consumers of cloud services have sufficient confidence in the market?
8. Is there a need for additional measures to raise awareness among consumers on what to look for in cloud service contracts? What form could these measures take?
9. What indicators should government look to, as evidence that there are consumer issues (such as systemic information asymmetry) in the cloud service market?

Chapter 3: Data protection and privacy

Discussion of issues

This chapter discusses a range of privacy issues that may apply in the cloud context, including ownership of data, applicable law, jurisdictional differences, cross-border disclosure, data loss, resilience and back-up data and data storage and deletion. This chapter also provides an overview of the new privacy regime under the *Privacy Act 1988* (Privacy Act) that will commence in March 2014 and examples of sector-specific privacy protections.

In the MYOB Business Monitor the key benefits identified by businesses using cloud services include access to data from anywhere (52 per cent) and the ability to work remotely (36 per cent)[61], indicating that the ability to have adequate access to data and services is a key issue for businesses in using the cloud. However, this must be balanced against adequate protection of personal information under the Privacy Act. Consumers have concerns about the existing privacy arrangements that apply to online services and this will continue to be an area of importance as more and more services move to the cloud.[62]

Research by Fujitsu has found that loss of, or unauthorised access to, data stored in the cloud is of concern to consumers worldwide.[63] Australians are particularly concerned about their privacy. Recent research undertaken by the Office of the Australian Information Commissioner (OAIC) indicates there is substantial community concern (90 per cent) about the practice of sending data overseas, with 79 per cent considering this a misuse of their personal information.[64]

These issues may be of relevance to all users of cloud services, whether individual, small business or not-for-profit consumers, and to many cloud service providers. As noted at the start of this stock take, the term 'consumer' includes individual, small business and not-for-profit consumers of cloud services, except where otherwise noted.

Privacy implications may vary substantially depending on the type of cloud service. As such, the issues discussed in this chapter may not apply to each type of service. For instance, the degree of interaction between a provider of infrastructure-as-a-service and their customers may be minimal and may raise limited personal data protection issues. In contrast, a provider of software-as-a-service may have more

---

[61] MYOB, *Business Monitor*, myob.com.au/myob/news-1258090872838?articleId=1257830858409, March 2013.

[62] According to the ACMA's Digital Footprints and Identities: Community attitudinal research, November 2013, 52 per cent of consumers lack confidence in existing privacy settings for online service providers, p 14.

[63] Fujitsu, *Personal Data in the Cloud: A global survey of consumer attitudes*, http://www.fujitsu.com/global/news/publications/dataprivacy.html, October 2010.

[64] OAIC, *Community Attitudes to Privacy Survey Research Report 2013*, www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013#_Toc368300726, October 2013.

interaction with its customers and potentially more associated personal data protection issues.[65]

In addition to data that is stored or accessed in the cloud, the use of digital technologies has created a growth in metadata, that is, data that relates to data. Metadata may include information such as the recipient of a communication, the author of an electronic document or the timing and length of a phone call. On the face of it, this data may not seem overly personal in nature, but may allow certain inferences to be drawn about relationships or an individual's circumstances.

Ownership of data

In the case of traditional ICT, the location of the servers will either be onsite or at another site, which is generally known to the customer, leading users to believe they have control over their data. In contrast, determining who owns the data in the cloud is not always a straightforward exercise. Generating, uploading, controlling or accessing information in a cloud does not necessarily equate with legal ownership.

There are circumstances in which the contract may seek to transfer ownership rights to the cloud service provider and consumers should consider the terms of the contract carefully. There may also be some instances in which the intellectual property rights in materials created under the contract vest in the cloud service provider because, for example, the provider has created a custom service for the customer.

Applicable law

The location of the data stored on a cloud service may have an impact on the laws that apply to that data, particularly privacy laws. With a cloud service there is potential for data to be stored in multiple jurisdictions, accessed and processed by multiple entities and the contract may not specify the physical location of storage facilities. As such, it is foreseeable that the laws of more than one jurisdiction could apply to the data because of the way it has been transmitted and stored.[66] This will have implications for both the obligations of the cloud service providers and users of cloud services, including individuals' rights to access and correct data.

Many Australian cloud service providers specifically reference their obligations under the Privacy Act in their terms and conditions.[67] Offshore-based cloud service providers make a general commitment to comply with applicable laws.[68] US-based providers tend to reference the US Safe Harbor scheme, although this would not apply to protect the data of Australian citizens.

While the contract may indicate that the cloud service provider applies the laws of another jurisdiction, this does not prevent a court from deciding that a business is

---

[65] D Vaile, K Kalinich, P Fair, A Lawrence, *Data Sovereignty and the Cloud*, Cyberspace Law and Policy Centre, UNSW Law Faculty, July 2013, p. 10.
[66] Ibid.
[67] M Vincent and K Crooks, *Cloud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 4.
[68] Ibid.

bound by Australian privacy law. The *Privacy Act 1988* includes provisions to provide extraterritorial operation, by extending it to organisations located outside Australia, but with an Australian link, that are collecting personal information in Australia (see discussion below under *Overview of existing regulation*). For business customers, to avoid the actions of the cloud service provider impacting on their business, they should be aware of the provider's privacy policies and may wish to make arrangements for the provider to agree contractually to apply Australian privacy principles to the storage of that information.[69]

Jurisdictional differences

Privacy is an area in which Australian law differs from the laws of some other major jurisdictions in two main ways that may impact on the way in which overseas providers offer services to Australian customers and the capacity of Australian-based cloud service providers to compete internationally. Firstly, in Australia, most small businesses are exempt from compliance under the Privacy Act.[70] Secondly, Australian privacy law does not distinguish between the degree of control an organisation has over personal information in the obligations placed on that organisation.

Under the EU Data Protection Directive, the personal information of EU citizens is unable to be transferred to another jurisdiction except where certain adequacy standards are met for the protection of data. Where the laws of a jurisdiction are not adequate, the EU has developed other mechanisms for ensuring that transfers of data can continue within the high standards set out in the Data Protection Directive. This includes the Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, the Binding Corporate Rules and the US-EU Safe Harbor Framework – see **Attachment D** for more information.

Australia's small business exemption under the Privacy Act is a major reason for Australian laws not being recognised as adequate by the EU.[71] In its 2008 review of privacy laws, the ALRC recommended that the small business exemption be removed.[72] The ALRC noted that removal of the exemption could facilitate trade with the EU. The Government has not yet responded to the ALRC's recommendation to remove the small business exemption.

A further area in which Australian privacy laws differ substantially from those of other jurisdictions is in the obligations imposed on 'processors of data'. The EU Data Protection Directive, the OECD Privacy Guidelines and the Asia Pacific Economic Cooperative (APEC) Privacy Principles differ to Australian law by distinguishing between data controllers and data processors. Data controllers – the consumers of cloud services – have the primary data protection obligations. Cloud service

---

[69] M Vincent and K Crooks, Cl*oud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 4.
[70] See section 6D of the Privacy Act for the definition of small business and exceptions to the small business exemption.
[71] ALRC, For Your Information: Australian Privacy Law and Practice, report 108, August 2008, p. 1328.
[72] Ibid, p. 1324.

providers would generally be considered data processors and would be subject to more limited obligations.

Under the EU Data Protection Directive, the obligations on data controllers are higher as they have collected the data for their own purposes, and will have the ability to access, update and use the data.[73] Data controllers generally have a relationship with the individual who is the subject of the personal information. Data processors, on the other hand, are subject to a limited range of obligations, principally focused on ensuring adequate security of personal information. The consequence is that cloud service providers in other jurisdictions may have more limited privacy obligations than under Australian law where all APP entities are required to comply with all APPs. Offshore-based cloud service providers may be unaware that Australian law does not distinguish between the degree of control that an organisation has over personal information.

The 2013 BSA Global Cloud Computing Scorecard, developed by BSA Software Alliance, a US-based advocate for the global software industry, assesses the readiness for cloud computing in various countries. The Scorecard notes that Australia has a comprehensive privacy regime in place, with no onerous registration system, although it notes that it is not compatible with the EU Data Protection Directive.[74] Further, the Privacy Act does not currently contain a specific data breach notification requirement.[75]

Cross-border disclosure

Depending on the type of service in use and degree of interaction and customisation, some cloud service providers may not take into account the needs of their business customers to comply with regulatory obligations or may be unaware of these obligations.[76] The cloud service provider may have no visibility of what is contained in the data stored on its service and whether there are legal implications, such as privacy, security or copyright. In addition, the cloud service provider may not know which data has been stored in which location, may lack the technical capacity to interrogate the data, or it may too costly to do so. This may mean that personal information stored in the cloud is not subject to adequate protections.

This may not differ substantially from traditional ICT services where the customer may use a service, such as renting server space or electronic language translation, and may not be aware of the precise location used to deliver the service. However, it

---

[73] J North and D Thompson, 'Privacy obligations of data processors: a conceptual gap affecting Australia's cloud industry', *Computers and Law*, No. 84, pp. 1-7, January 2013.
[74] BSA Software Alliance, *Global Cloud Computing Scorecard*, cloudscorecard.bsa.org/2013/, 2013.
[75] The Privacy Act may require notification where it is a reasonable step to protect personal information from misuse, interference and loss, or from unauthorised access, modification or disclosure under the requirements of Australian Privacy Principle 11. Further, the *Personally Controlled Electronic Health Records Act 2012* imposes mandatory data breach notification obligations for certain kinds of data breaches involving the e-health system.
[76] W Kuan Hon, C Millard and I Walden, 'Negotiating the cloud: Looking at clouds from both sides now', *Stanford Technology Law Review*, Vol. 16, No. 1, Fall 2012, p. 98.

may be of particular concern for business customers that need to comply with privacy laws that prevent or limit the disclosure of personal information across borders.

Contracts may permit the transfer of data to other jurisdictions, with or without the consent of the customer.[77] In some cases, the customer may be able to specify if not the country then at least the region or regions in which data will be stored.[78] This is an area in which some cloud service providers may seek to differentiate themselves by ensuring that Australian data centres are used. Businesses should be aware of their obligations in regards to cross-border disclosure of personal information under the Privacy Act.

Some providers may be willing to meet additional contractual obligations where necessary due to the nature of the data stored, although it is likely that further costs would be imposed.[79]

It is noted that individual consumers may also have concerns about the location in which their data will be stored and may wish to check this with the cloud service provider.

Data loss

Loss of data, for example, through a change in the provider's circumstances, such as the services offered, insolvency or sale or, in the unlikely event of the service being discontinued due to law enforcement action (such as in the Megaupload case) can be a significantly disruptive process for a customer. The customer may have limited ability to retrieve their data and transition to another provider to ensure ongoing provision of service to their customers or access to their data.

Data loss in the cloud

In January 2012, US authorities shut down Megaupload, a New Zealand based cloud storage service, following allegations that the service was used to store copyright infringing material. Users of the service were unable to retrieve their data for a period of time, even where that data did not contain copyright infringing material.

These issues highlight the importance of having a redundancy plan, where copies of data may be stored in a separate and readily accessible location, in place to ensure that the impact on a user is minimised.[80]

An overseas cloud service provider, even if it is carrying on business in Australia, will often be incorporated in another jurisdiction and the laws of that jurisdiction will apply to a winding up of the company. This may create issues for a customer of a

[77] M Vincent and K Crooks, *Cloud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 5.
[78] Ibid.
[79] Ibid, p. 4.
[80] D S Caplan, 'Bankruptcy in the Cloud: Effects of Bankruptcy by a Cloud Services Provider', *The Senior Lawyer*, Spring 2012, Vol. 4, No. 1, p. 18.

cloud service in accessing data stored in that service.[81]

Resilience and back-up data

Threats to the continuity of service may arise from a network outage or interruption, hardware or software failure, a power failure or a natural disaster.

Cloud service providers should have appropriate resilience arrangements in place to ensure that data is available in the event of a service outage, for example, by having data backed up at another location or having an alternative means of accessing data in the event of an outage. Additionally, appropriate security and data segregation should be provided for the backed up data to ensure that the same protections that apply to the original copy of data also apply to the back-ups.

Data storage and deletion

Data must be stored in such a way that the customer can effectively comply with obligations, such as discovery for litigation or maintaining the currency of personal information under privacy laws[82], and that there are arrangements in place to ensure that law enforcement agencies can access data where required or authorised by law. In addition, Australia has approximately 450 pieces of legislation dealing with data storage for different purposes, in areas such as taxation, workplace relations, corporations law and telecommunications.[83]

The ability to have data deleted once it is no longer required[84], or at the completion of the contract, is also important. In particular, deletion of data after termination of service ensures there are no ongoing privacy or security implications, particularly since there may be no obligation for the cloud service provider to maintain the security of the data once the contract has ended.

Research on key terms in cloud service contracts indicated that few contained 'strong provisions requiring the provider to assist with transition out and/or the recovery of the data, even at an additional cost.'[85] Some of the contracts allowed a transitional period to migrate data to another system, of between 15 to 90 days. The terms that did provide for assistance were of a highly discretionary nature. Some of the contracts also indicated data would be deleted within a certain timeframe, sometimes this was limited to data identified as containing personal information. Other contracts only provided for deletion at the discretion of the provider.

---

[81] D S Caplan, 'Bankruptcy in the Cloud: Effects of Bankruptcy by a Cloud Services Provider', *The Senior Lawyer*, Spring 2012, Vol. 4, No.1, p 16.

[82] Visit www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles for more information, see APPs 12 and 13 in the OAIC fact sheet.

[83] A Wong, *Understanding the legal framework of moving to cloud computing*, Speech to CeBIT, www.slideshare.net/CeBITAustralia/cloud-computing-conference-2011-anthony-wong-acs, 31 May 2011.

[84] Visit www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles for more information, see APP 11.2 in the OAIC fact sheet.

[85] M Vincent and K Crooks, *Cloud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 15.

Overview of existing regulation

In Australia, privacy protections are provided through the Privacy Act and other supporting legislation that deals with specific industries. Some examples of industries that have specific privacy protections are the telecommunications industry and the health services sector. There is also state and territory privacy legislation, which is broadly consistent with the Privacy Act.

The Privacy Act sets out protections for the privacy of individuals by imposing obligations on certain entities that collect, store or process personal information. Changes to the Privacy Act came into effect on 12 March 2014, including the introduction of a single set of APPs that apply to all entities covered by the Privacy Act ('APP entities').[86] This replaces the Information Privacy Principles (IPPs) that applied to public sector organisations covered by the Privacy Act and the National Privacy Principles (NPPs) that applied to private sector organisations covered by the Privacy Act.

Key concepts

This section discusses some of the key concepts used in the Privacy Act. Some of these concepts are not defined in the Privacy Act and, as such, the OAIC has issued APP Guidelines providing guidance on its interpretation of a range of key concepts in the new APPs.[87]

What is personal information?

Under section 6 of the *Privacy Act 1988* personal information means '... information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.'

APP entity

An APP entity is defined as an agency or organisation.[88] 'Agency' includes Commonwealth government agencies, the Norfolk Island Government and certain bodies or tribunals established or appointed for a public purpose by or under Commonwealth legislation. The reforms do not apply to government agencies in the Australian Capital Territory, where the IPPs will continue to apply.

'Organisation' is defined to include individuals, body corporates, partnerships, unincorporated associations and trusts, other than small business operators.[89]

Small business operators, with annual turnover of $3 million or less for a financial

[86] Visit www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles for more information, see APP 11.2 in the OAIC fact sheet.
[87] Visit www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/ to view the APP Guidelines.
[88] Subsection 6(1) of the Privacy Act.
[89] For more information, see OAIC, APP Guidelines, Chapter B: Key Concepts, February 2014, p 3.

year, are exempt from the Act.[90] A small business operator can elect to be covered by the provisions of the Privacy Act.[91] Some businesses are covered by the Privacy Act even where they would otherwise meet the definition of a small business operator, including businesses that:

- provide a health service and hold health information other than in an employee record
- disclose personal information for a benefit, service or advantage
- provide a benefit, service or advantage to collect personal information.[92]

Australian link

The Privacy Act extends to an act done, or a practice engaged in, outside of Australia by an organisation that has an Australian link.[93] For an organisation or small business operator to have an Australian link (and, therefore, be subject to the Privacy Act) it must be:

- an Australian citizen or person whose continued presence in Australia is not subject to a time limitation imposed by law
- a partnership formed or, a trust created, or a body corporate incorporated, in Australia or an external territory, or
- an unincorporated association that has its central management and control in Australia or an external territory (subsection 5B(2)).

When an organisation (bound by the Privacy Act) does not fall within one of the above categories, it will still have an Australian link where it carries on business in Australia or an external territory and the personal information was collected or held by the organisation in Australia or an external territory either before or at the time of the act or practice.[94] Carrying on business in Australia applies to circumstances in which the business does not have a physical presence in Australia but conducts activity in Australia that forms part of its business. This may include where it collects personal information from individuals located in Australia or offers goods or services to individuals in Australia.[95] It should be noted this is based on the OAIC's interpretation in its APP Guidelines. Whether an overseas business will be considered bound by the Privacy Act is ultimately a question for the court.

There are three main instances in which privacy laws may be applicable to cloud services:

---

[90] See section 6C of the Privacy Act for the definition of a small business operator.
[91] Section 6EA of the Privacy Act.
[92] See section 6D of the Privacy Act for the full list of exemptions.
[93] Subsection 5B(1A) of the Privacy Act.
[94] Subsection 5B(3) of the Privacy Act.
[95] For more information see OAIC, APP Guidelines, Chapter B: Key Concepts, February 2014, p 5 and the Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

- a business bound by the Privacy Act is storing or accessing the personal information of its customers in the cloud
- a cloud service provider bound by the Privacy Act is storing or accessing personal information on its customers, or
- a cloud service provider bound by the Privacy Act is storing or accessing personal information on the customers of one of its customers.

Collects

Subsection 6(1) defines 'collection' as circumstances in which an APP entity collects personal information for inclusion in a record or in a generally available publication. Collection 'includes gathering, acquiring or obtaining personal information from any source or by any means'.[96] A record is defined in subsection 6(1) to include a document or an electronic or other device.

Holds

Subsection 6(1) defines 'holds' as circumstances in which an APP entity has possession or control of a record containing personal information.[97] This extends both to circumstances in which an entity physically possesses a record containing personal information or where it has the right or power to deal with the information, even when the information is physically possessed or stored by another entity. For example, an APP entity will still hold information that is stored on servers or in a cloud service owned by a third party, provided the entity has the ability to access and amend the information.

Use versus disclosure

'Disclosure' is not defined in the legislation, however, the APP guidelines indicate that a disclosure will generally occur where an organisation releases personal information from its effective control and makes it accessible to someone outside the organisation.[98]

'Use' is also not defined in the legislation. An APP entity will generally use personal information when it handles and manages the information within the entity's effective control.[99]

The APP Guidelines indicate that the provision of personal information to a contractor will generally amount to a disclosure.[100] However, there are limited circumstances in which it may be considered a use. For example, where an APP entity provides personal information to a cloud service provider for the limited purposes of storing the information and giving access to the entity, it may be a use of

[96] See discussion of 'collects' in OAIC, APP Guidelines, Chapter B: Key Concepts, February 2014, p. 6.
[97] See discussion of 'holds' in OAIC, APP Guidelines, Chapter B: Key Concepts, February 2014, p. 17.
[98] See discussion of 'disclosure' in OAIC, APP Guidelines, Chapter B: Key Concepts, February 2014, p. 12.
[99] See discussion of 'use' in OAIC, APP Guidelines, Chapter B: Key Concepts, February 2014, p. 27.
[100] OAIC, APP Guidelines, Chapter B: Key Concepts, February 2014, p. 13.

personal information, rather than a disclosure, provided:

- there is a binding contract that requires the cloud service provider to handle the personal information for the limited purposes of storage and providing access to the entity
- the contract obliges any subcontractors to handle the personal information in the same way
- the contract gives effective control to the entity about how the personal information is managed by the provider. There are certain issues to consider including, whether the entity retains the right and power to access, change or retrieve the information, who else can access the information and for what purpose, the security measures that apply to the storage of the information and whether the information can be retrieved or permanently deleted at the completion of the contract or when it is no longer required.[101]

Overview of APP requirements

This section discusses certain aspects that may have particular significance in the cloud environment, noting that the relevance of the APPs will vary depending on the specific business arrangements and all may be relevant.[102]

While the discussion focuses on the obligations of businesses and cloud service providers bound by the Privacy Act, many of the privacy protections in the Privacy Act will have broader relevance to individual consumers of cloud services in considering the extent to which a provider will apply privacy protections to their personal information. Similarly, while some small business and not-for-profit consumers may not be bound by the Privacy Act, they will still have an interest in ensuring the personal information of their customers or clients is protected in the cloud environment. Aside from the possibility of being the subject of an investigation for breach of the Privacy Act, inadequate privacy practices in storing data in the cloud could result in significant reputational damage for small businesses, not-for-profit organisations and cloud service providers.

APP 1 requires an entity to have practices or policies in place that will ensure that the entity complies with the APPs, will enable it to deal with complaints about privacy and set out how it will manage personal information.

APP 5 requires notification of certain matters to an individual at the time of collection of personal information, including if the information is likely to be disclosed to overseas recipients and the countries in which they are likely to be located, where practical to do so (APP 5.2 (j)).

An important aspect of the privacy reforms was to update the law on cross-border transfers of information, moving from an adequacy approach to an accountability

[101] Ibid, p. 28.
[102] Visit www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/ for detailed information.

approach, consistent with the APEC Privacy Framework 2004.[103] This is also consistent with the OECD Privacy Principles. The inclusion of APP 8 and section 16C in the Privacy Act, represents a significant change from the previous NPP 9, which set out certain circumstances in which personal information could be transferred. For consistency with state and territory privacy laws, APP 8 refers to the 'disclosure' of information, while NPP 9 applied to 'transfers' of information.[104] 'Transfer' was not defined, but referred to the movement from one place or application to another and was potentially broader in its application than the disclosure of information.

APP 8.1 requires an APP entity to take reasonable steps before it discloses information to ensure that an overseas recipient to whom personal information is disclosed does not breach the APPs in relation to the information.[105] Generally this means there is an obligation on the APP entity to ensure that the overseas recipient will handle an individual's personal information in accordance with the APPs.

Section 16C extends the application of the Privacy Act in circumstances in which an APP entity discloses personal information to an overseas recipient that is not bound by the Privacy Act and the recipient breaches an APP (other than APP 1). In these circumstances the act is taken to have been done by the APP entity and they would be liable for the breach.

APP 8.2 sets out a range of exceptions to the requirement in 8.1 and section 16C, including where:

- the entity reasonably believes that the recipient is subject to a law or a binding scheme that provides protections that are substantially similar to the protections provided under Australian law and there are mechanisms to enable an individual to take action to enforce those protections
- the entity expressly informs the individual that if they consent to the disclosure, APP 8.1 will not apply and the individual consents to the disclosure with this in mind
- the disclosure is required or authorised by Australian law
- the disclosure is a permitted general situation as provided for in the Act (section 16A)
- the entity is an agency and the disclosure is required or authorised under an international information sharing agreement to which Australia is a party, or
- the entity is an agency and believes the disclosure is reasonably necessary for law enforcement purposes and the recipient is a body performing functions or exercising powers similar to those performed or exercised by an enforcement body.

[103] Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012.
[104] Ibid.
[105] For more information on the operation of APP 8, see Chapter 8 of OAIC, APP Guidelines, February 2014, p 3.

However, even where an exception in 8.2 applies, there is still a requirement to ensure the security of personal information consistent with APP 11.

Whether storing information on a cloud service will be considered a disclosure may depend on the specific circumstances of the service, including the capacity of the service provider to view and access the data.[106] The disclosure of personal information is relevant to a range of APPs, including APP 1.4 (under which an entity must include information about the locations to which disclosure may occur in its privacy policy) and APP 5.2 (under which an entity must advise an individual at the time of collection that the personal information may be disclosed overseas). It may be difficult for customers to meet their requirements under APPs 1.4 and 5.2 as the location of data may not be advised by the cloud service provider.

In any event, whether or not the use of cloud services to store personal information constitutes a use or a disclosure, the customer, if an APP entity, would be 'holding' the personal information and would need to comply with the APPs.

Issues may also arise with the capacity of a business customer to access, review or update the personal information stored in a cloud service quickly and easily in order to meet its privacy obligations. APP 10 requires an entity to take reasonable steps to ensure that personal information collected, used or disclosed is accurate, up-to-date, complete and (for use and disclosure) relevant. APP 12 requires an entity to give an individual access to personal information held about them, following a request from the individual. APP 13 requires an entity to correct personal information held on an individual, following a request from the individual. The capacity to meet obligations under these APPs will depend on the service being used and the ability of the customer to readily access and alter the personal information that is stored in the service. In particular, the way in which data is backed up and deleted by the service could create difficulties in complying with these obligations. As these obligations apply to back-ups of data as well, there may be instances in which out-dated data continues to be backed up on a service, possibly in breach of APP 10 or 12. This may be a back-end process, of which the cloud service customer is unaware. Potentially the cloud service provider is also unaware that personal information subject to the Privacy Act is stored on their service. This highlights the need for business consumers to ensure that a cloud service is suitable for their needs in allowing them to satisfy privacy obligations.

APP 11.1 requires an entity to take reasonable steps to ensure that personal information is protected from misuse, interference or loss and from unauthorised access, modification or disclosure. APP 11.2 requires an APP entity to take reasonable steps to delete or de-identify personal information that is no longer needed for the purpose for which it was collected (or required to be retained by law). 'Reasonable steps' may include having contractual arrangements in place to ensure that any third party undertaking the storage and management of personal information will delete or de-identify the information as per the customer's request. A number of provider contracts fail to specify the deletion of personal data on the

[106] See discussion of 'use' in OAIC, APP Guidelines, Chapter B: Key Concepts, February 2014, p 28.

termination of service.[107]

Cloud computing, as with traditional ICT outsourcing, does not enable an entity to avoid its responsibilities under privacy laws. APP 11 would apply to circumstances in which an entity uses a cloud service to store data but does not take reasonable steps to ensure that the data is secured by the cloud service provider. In obtaining cloud services, a business customer should consider whether the arrangements for storing personal information in that service are consistent with its privacy policies and should review the privacy policy (if any) of the cloud service provider. Customers may also seek to negotiate terms with the cloud service provider to oblige them to comply with Australian privacy laws (noting, of course, that in practice they may have limited capacity to negotiate terms with cloud service providers and many other large ICT providers).

Australian privacy laws may have an impact on competition in the Australian cloud services market, in the event that overseas providers are unwilling to contractually agree to comply with Australian privacy laws, as Australian cloud services providers will already be required to comply with the laws and may be less likely to store data in an overseas jurisdiction.

From March 2014 the Australian Information Commissioner will have enhanced enforcement powers, which will generally be exercised by the Privacy Commissioner, including the ability to:

- accept enforceable undertakings
- seek civil penalties in the case or serious or repeated breaches
- conduct assessments of privacy performance of APP entities.

Privacy protections in other industries

In addition to the protections provided under the Privacy Act, a range of industries have additional regulation, due to the amount or sensitivity of information which is processed, including the telecommunications industry, health services industry and financial services industry.

Part 13 of the Telecommunications Act protects telecommunications information obtained by carriers, carriage service providers, emergency call persons, number database operators and their respective associates (including employees and contractors) during the supply of telecommunications services. While cloud service providers are not specifically covered by the Telecommunications Act, there may be circumstances in which the nature of services provided means that a cloud service provider will be a carriage service provider and subject to the obligations in the Telecommunications Act. More discussion on this point is contained in Chapter 2.

The Telecommunications Act requires regulated entities to protect the confidentiality of information relating to the contents of communications carried,

[107] M Vincent and K Crooks, *Cloud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 15.

carriage services supplied, and the affairs or personal particulars of persons (protected information). The privacy protections in Part 13 of the Telecommunications Act recognise that the content of communications and information related to its transmission can be highly sensitive. One feature of the Part 13 scheme is that it can apply to small businesses that may not be subject to the Privacy Act because of the small business exemption. The Telecommunications Act scheme also creates a series of criminal offences for unauthorised disclosures and uses of information.

Exemptions apply to allow the disclosure or use of protected information under Part 13 in certain circumstances, such as performance of duties, law enforcement, investigation of a complaint, emergency service calls, preventing or lessening a serious or imminent threat or where it is done with the knowledge or consent of the individual concerned. Disclosure or use of information must be for an authorised purpose. The Telecommunications Act also requires regulated entities to report disclosures of information to the ACMA and maintain adequate records of disclosures. The Information Commissioner can monitor compliance with Part 13 of the Telecommunications Act.

The *Telecommunications (Interception and Access) Act 1979* also has the effect of protecting the privacy of individuals by prohibiting the interception of communications passing over a telecommunications system, and access to stored communications held by a carrier, except in certain circumstances. More information on this legislation is provided in Chapter 6.

Due to the potential sensitivities involved in medical information, there is also additional regulation of the health services industry. For example, the *Personally Controlled Electronic Health Records Act 2012* sets out arrangements for a scheme under which individuals can establish an e-health record which can be shared with chosen health care providers. The scheme includes rules relating to the security and privacy of e-Health records. A requirement of the scheme is that records must be stored within Australia, it cannot be taken, held, processed or handled outside Australia except where the record does not contain any personal or identifying information about participants within the e-health record system.

Potential Triggers

The nature of cloud services may make it difficult for both providers and business customers to understand their obligations and rights. For those providers servicing customers in multiple jurisdictions, it may be particularly difficult to determine a privacy policy that will provide adequate and practical protections for their customers' needs given the differences in privacy laws between jurisdictions.

Currently under Australian law, there is limited legislative protection for return of data in the event that a cloud service is shut down. The *Corporations Act 2001* provides some protections for creditors who are owed money by a company that is subject to insolvency proceedings, but does not provide explicit rights to consumers whose data is being held by a third party. A common law right either under bailment or under the contract may apply, but in practice it may be difficult for a consumer to

enforce these rights against the company or relevant insolvency practitioner. This may be more so where the service provider is based overseas and subject to insolvency laws in another jurisdiction.

Notification of security breaches relating to personal information may be an area of importance in ensuring that data is adequately secured and protected in the cloud, as well as preventing subsequent breaches through changes to practices, where necessary. There is currently no data breach notification regime in Australia. This was a recommendation of the ALRC's 2008 privacy inquiry.[108] Legislation to establish such a scheme was introduced to Parliament in May 2013, but lapsed due to the election being called.[109] The Government is considering its position on a Commonwealth mandatory data breach notification scheme. Few cloud service contracts provide for notification in the event of a data breach.[110] The OAIC has issued guidance on the voluntary notification of breaches.[111]

Triggers that may indicate serious issues with privacy in the Australian cloud services market may include:

- **Low adoption because of privacy concerns:** Low adoption rates among individual consumers compared to other jurisdictions could indicate they are concerned about the privacy of their information stored in the cloud. Consumer surveys could be used to determine whether privacy was the key issue of concern. Low rates of adoption among small business or not-for-profit consumers may indicate that they do not understand or hold concerns over their privacy obligations when storing information in the cloud. A high number of requests for changes from standard contract terms to specifically address Australian privacy laws may also indicate that jurisdictional differences are impacting on the take up of cloud services.

- **Complaints data:** A high number of complaints to the OAIC or the ACMA could be indicative that cloud service providers do not understand their obligations under Australian privacy law or incorrectly consider themselves not subject to Australian law. Further, if regulators are unable to effectively enforce obligations against cloud service providers based overseas, this may limit the protections available to consumers and may in turn reduce confidence in the cloud services market generally.

- **Consumers do not understand how to make a complaint:** Referral of privacy complaints to the incorrect regulator may indicate that consumers need better education about privacy protections and how to initiate a complaint.

---

[108] ALRC, For Your Information: Australian Privacy Law and Practice, report 108, August 2008, Recommendation 51-1.
[109] The bill was entitled the Privacy Amendment (Privacy Alerts) Bill 2013.
[110] M Vincent and K Crooks, *Cloud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 11.
[111] OAIC, Data Breach Notification – A guide to handling personal information security breaches: www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches, April 2012.

Conclusion

Privacy in the online environment is an area of significant concern to consumers, both in terms of their own personal information and, for business customers, in terms of protecting the personal information of their customers. As personal information moves to the cloud, there is a need to ensure that adequate privacy and security settings are in place.

Chapter 3 Questions

10. Are there other issues that affect data protection in cloud services?
11. Are existing privacy protections suitably tailored to cloud services? Do cloud services raise novel issues in the application of privacy law?
12. Are there areas of privacy law that would benefit from further clarification?
13. To what extent are jurisdictional differences between privacy regimes creating problems in the take up or provision of cloud services in Australia?
14. What are the benefits to Australian consumers in using onshore data centres? What are the benefits of offshore data centres?
15. What indicators should government consider to determine whether there are significant privacy concerns in the Australian cloud services market?

Chapter 4: Cybersecurity

Discussion of issues

This chapter discusses Australia's approach to cybersecurity and the potential impact of cybercrime and security arrangements on cloud computing. This chapter provides an overview of the application of the *Cybercrime Act 2001* (Cybercrime Act), *Crimes Act 1914* (Crimes Act) and the *Criminal Code Act 1995* (Criminal Code).

For small businesses and not-for-profit organisations cloud computing can often improve security settings and expertise. The scale of cloud service providers often means that they have more resources with which to prevent security threats than may be the case with traditional ICT. A Microsoft study of 106 US-based small to midsize businesses found that most (94 per cent) of those businesses using cloud had experienced security benefits, including more up-to-date anti-virus software and better spam filters.[112] Of those surveyed, 91 per cent found an overall improvement in their security settings because of their use of the cloud and an improvement in their ability to comply with obligations.

What is cybersecurity?

The Australian Government defines cybersecurity as:

'Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.'

Source: Australian Government Cyber Security Strategy 2009

Despite these benefits, consumers remain concerned about security in the cloud. The same Microsoft study found that security concerns continue to be a key barrier to take up (60 per cent of respondents), along with the perceived lack of control over data (45 per cent of respondents) and the ability to comply with obligations (39 per cent).[113] Of those respondents that did not use cloud computing, 32 per cent said the introduction of industry standards on security would encourage them to consider its adoption.

The 2013 Unisys Security Index found that unauthorised access to or misuse of data is a top security concern for 62 per cent of Australians.[114] The loss of or the unauthorised access to data stored in the cloud is of particular concern to ICT security specialists.[115] In addition, Fujitsu found this of concern to consumers worldwide, with 88 per cent of survey respondents concerned about who has access

[112] Microsoft, *Small and midsize businesses cloud trust study: US study results*, www.microsoft.com/en-us/news/download/presskits/security/docs/twcjune13us.pdf, June 2013.
[113] Ibid.
[114] Unisys, Security Index Australia, www.unisyssecurityindex.com/usi/australia, May 2013.
[115] A Aleem and C R Scott, 'Let me in the cloud: analysis of the benefit and risk assessment of cloud platform', *Journal of Financial Crime*, 2013, Vol. 20, Issue 1, pp. 6-24.

to personal information.[116]

Cybercrime

Cybercrime relates to both crimes that are directed at computers or other ICT and crimes that use computers or ICT as an integral part of the offence.[117] There have been examples of cloud services being used to host criminal activity, such as storage or distribution of exploitative material and stolen personal information.[118] A cloud service could also be used for botnet activity, where computers infected with malware are used for distributing spam or scam emails and for denial of service attacks. This could open up other users of the cloud service to potential security breaches or the possibility of loss of data and service if the service is shut down by a law enforcement agency and data is seized.

In many respects, cloud computing faces the same security threats as other online services, including phishing, domain name system attacks, session hijacking, distributed denial of service attacks, or simply poor security processes, such as faulty authentication checks.[119] These are not necessarily new concerns and rather than discouraging the use of cloud computing, there is a need to ensure appropriate security settings are in place to address these issues.

The 2013 BSA Global Scorecard notes that Australia scores well on its approach to cybercrime, with the ratification of the Cybercrime Convention.[120] Although, it notes there are limited general security requirements for cloud services and no specific security audit arrangements.[121]

Security

Public cloud offerings that use a co-tenant or multi-tenant arrangement may raise particular security concerns as there may be more scope for data to be accidentally or intentionally accessed by other tenants and difficulties in imposing custom security settings for each user.[122]

A further security issue that customers should be aware of is whether their provider will notify them if a security breach occurs. Such notification could usefully include when it occurred, the unauthorised party, what information was accessed or potentially accessed, possible means of redress by the customer and arrangements

---

[116] Fujitsu, *Personal Data in the Cloud: A global survey of consumer attitudes*, www.fujitsu.com/global/news/publications/dataprivacy.html, October 2010.
[117] Attorney-General's Department, *National Plan to Combat Cybercrime*, www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx, July 2013, p. 4.
[118] A Hutchings, R G Smith and L James, 'Cloud computing for small business: Criminal and security threats and prevention measures', *Trends and issues in crime and criminal justice*, No. 456, Australian Institute of Criminology, May 2013.
[119] Ibid.
[120] BSA Software Alliance, *Global Cloud Computing Scorecard*, http://cloudscorecard.bsa.org/2013/, 2013, p. 7.
[121] Ibid, p. 16.
[122] M Vincent and K Crooks, *Cloud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 7.

the service provider has put in place to prevent future instances of access.

Security settings will generally be set out in the cloud services contract or other supporting documentation. Some contracts only require 'reasonable' or 'appropriate' measures to be in place or establish a baseline level for security (such as compliance with certain technical standards).[123]

Security arrangements must be adequate to ensure there is no unauthorised access to the data stored on a cloud service or the data transferred to or from the service, whether by the cloud service provider, by other customers of the provider or by third parties. Not only can data loss have a significant impact on the ability to carry on business, it could also leave the customer open to legal claims from its clients or enforcement action by regulators, as well as having an impact on reputation.

Both the cloud service provider and the customer have a role to play in ensuring adequate security is maintained. Some providers may require the customer to ensure that it has adequate security settings in place to secure data.[124] As cloud services are more mobile, capable of being accessed from anywhere and from any device, strong password practices become a more significant preventative measure.[125] In addition, cloud service providers should have adequate internal security practices in place, including maintenance of physical facilities, security checks for staff, adequate authentication processes and encryption of stored and transmitted data.

Many cloud service providers will comply with ISO 27001[126] and SSAE 16 SOC1/2[127], international standards which set security requirements. There are also a range of industry-led initiatives to create best practice in security. These include the Cloud Security Alliance's Security, Trust and Assurance Registry. This initiative aims to encourage transparency in security arrangements by enabling cloud providers that meet certain security benchmarks to be included on the registry without cost. Consumers can search the registry, also without cost, to check whether a cloud service provider meets certain security standards. Registration is through completion of a questionnaire and a basic security check.

Similarly Microsoft is due to launch its Security Assessment for Evaluation (SAFE) program. This will provide businesses with information about how to meet

---

[123] M Vincent and K Crooks, *Cloud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 8.
[124] Ibid, p. 7.
[125] A Hutchings, R G Smith and L James, 'Cloud computing for small business: Criminal and security threats and prevention measures', *Trends and issues in crime and criminal justice*, No. 456, Australian Institute of Criminology, May 2013.
[126] The full name is ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements. It is an information security management system standard developed by the International Organization for Standardization and the International Electrotechnical Commission.
[127] The full name is Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization. It was created by the Auditing Standards Board of the American Institute of Certified Public Accountants.

compliance obligations and manage risks in the cloud.

Cyber liability insurance is a growing area and may be available to protect consumers against the risks associated with doing business in the digital economy, although it will not prevent a consumer from potential breach of relevant legislation, such as the Privacy Act.

Overview of existing regulation

The Cybercrime Act introduced new offences into the Criminal Code relating to the misuse of computers and telecommunications systems, replacing the out-dated offences in the Crimes Act. The Criminal Code covers a range of offences, including hacking, denial of service and malware. The Criminal Code makes it an offence to cause the unauthorised access, modification or impairment to data held in a computer with the intent to commit a serious offence against a law of the Commonwealth, a state or territory. A serious offence is one punishable by imprisonment of five years or longer. It is also an offence to possess or control data, or to produce, supply or obtain data with the intent to commit a computer offence.

Further amendments to Australia's cybercrime laws were introduced by the *Cybercrime Legislation Amendment Act 2012*, which enabled the Council of Europe Convention on Cybercrime (the Convention) to come into effect for Australia on 1 March 2013. It sets out new investigative powers to assist law enforcement agencies in pursuing cybercrime and working with international counterparts. The legislation was necessary to facilitate Australia becoming a party to the Convention.

Under the legislation, law enforcement and intelligence agencies can compel carriers to preserve communications records relating to both domestic and foreign cybercrimes through a preservation notice. A stored communications warrant is required before the agency can access the communications records. Additional privacy protections and reporting requirements apply to the new powers.

The legislation also expanded the computer offences in Part 10.7 of the Criminal Code Act to meet the obligations set out in the Convention. Specifically, it removed the requirement that a Commonwealth computer, Commonwealth data or a carriage service be involved in or affected by the conduct constituting the offence. The legislation also clarified that the computer offences apply to conduct occurring wholly or partly in Australia or on board an Australian aircraft or ship (as required by the Convention). In some circumstances, the offence may extend to the conduct of Australian nationals in an overseas jurisdiction.

There is some crossover between cybersecurity and the Government access regime discussed in Chapter 6. Subsection 313(1) of the Telecommunications Act requires carriers and carriage service providers to do their best to prevent their network or facility being used in connection with offences against the Commonwealth or a State or Territory. Subsection 581(3) of the Telecommunications Act enables the Attorney-General (in consultation with the Prime Minister and the Minister for Communications) to direct a carrier or carriage service provider to not use or supply, or to cease using or supplying, carriage services if the use or supply is considered prejudicial to security. Such a direction cannot apply to the supply of carriage

services to a specific person or a class of persons.

The Privacy Act contains an exemption to allow the disclosure of personal information to a law enforcement agency where the cloud service provider reasonably believes that the use or disclosure is reasonably necessary to prevent, detect, investigate, prosecute, or punish violations of law or serious breaches of standards of conduct, including corruption, abuse of power, dereliction of duty or seriously reprehensible behaviour.

The legal framework for cybercrime has been updated to enable computer-based crimes to be more effectively caught. However, there remains some uncertainty about the extent to which a crime that occurs on a cloud service would be caught by the provisions of Australian cyber laws. This is because the Criminal Code refers to 'access to data held in a computer[128]', which means:

> '(a) the display of the data by the computer or any other output of the data from the computer; or
>
> (b) the copying or moving of the data to any other place in the computer or to a data storage device; or
>
> (c) in the case of a program—the execution of the program.'

Further, cross-jurisdictional issues may create some complexities in determining where an offence has occurred and whether it amounts to a breach of Australian law.

As noted in the National Plan to Combat Cybercrime,

> While Australia's current legal frameworks effectively cover the range of conduct that constitutes cybercrime, it is important that new technologies do not allow criminals to exploit loopholes.[129]

Under the current regulatory environment there is no enforceable obligation on telecommunications owners and operators to protect their networks and facilities, as the Telecommunications Act requires them to 'do their best'. Existing regulatory arrangements do not require industry to build national security considerations into their business and investment decision making.

The Parliamentary Joint Committee on Intelligence and Security undertook a review of national security legislation, handing down its report in June 2013. A recommendation of the Committee's report (recommendation 19) is to introduce a security framework that would have the effect of requiring industry to ensure adequate oversight and control of its infrastructure and data held and carried across it. This could be achieved, for example, by industry demonstrating competent supervision and effective control when using third party cloud service providers.

---

[128] Paragraph 476.1 of the *Criminal Code Act 1995*.

[129] Attorney-General's Department, *National Plan to Combat Cybercrime*, www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx, July 2013, p. 21.

Potential triggers

Some potential triggers that security arrangements may be inadequate in the cloud services market may include:

- **Cloud service providers are not taking adequate steps to secure networks:** Failure to effectively manage the security of networks could have a significant impact on Australia's national security, affecting government, business and individuals by allowing security weaknesses to be exploited. Inadequate security measures may be evidenced by a rise in complaints to the ACCC, ACMA, OAIC or other enforcement bodies or even by high profile breaches reported in the media. This could also be measured through investigations by relevant law enforcement agencies and broader reviews of Australia's national security arrangements for its ICT and telecommunications systems.
- **Existing regulatory arrangements do not adequately cover cybercrime occurring in the cloud:** Representations from law enforcement agencies could indicate that the existing regulatory or practical arrangements are insufficient.
- **Difficulties in understanding security arrangements:** If consumers were experiencing problems understanding the existing security measures applied by providers, this may lead to reduction in consumer confidence. Consumer understanding of security arrangements in place could be measured through consumer surveys and complaints data.

Conclusion

Australia's national security has implications for individuals, business, government and the broader economy. Concerns over the security of cloud systems have the potential to affect consumer confidence in using cloud services. There is potentially a role for government in encouraging cloud service providers to ensure the security of their systems and to require certain security standards are met in the storage of government data. Industry also has a significant role in developing and implementing appropriate security measures for their systems and in continuing to enhance these systems over time to respond to emerging threats.

Chapter 4 Questions

16. Are there other cybersecurity issues that affect cloud computing?
17. Are existing laws adequate in protecting users of cloud services? What opportunities exist to promote even greater confidence in the cloud services market?
18. What indicators should government consider to determine whether there is a lack of adequate security in the cloud services market?

Chapter 5: Government use of cloud computing

Discussion of issues

This chapter discusses the impact of government use of cloud computing on the cloud services market more broadly and the application of existing government policies, including outsourcing and offshoring policies, and the Commonwealth Procurement Rules.

A key driver for the take up of cloud services among small business and the not-for-profit sector is the increased use of cloud services by government agencies. With annual ICT procurement of over $5 billion, the Australian government is well-placed to provide leadership on the appropriate adoption of cloud computing.[130]

As the government increases its use of cloud services, the way government agencies contract for cloud services may influence the terms and conditions offered to Australian consumers of these services more broadly. Australian providers may seek to differentiate their services on issues of particular concern to consumers, such as best practice security and privacy arrangements, including onshore storage of data.

The government recognises that it has a role in being a model user of cloud services, and that it must adopt cloud in a way that appropriately considers privacy and security questions. The government has indicated its focus on reducing the cost of ICT use by government and increasing productivity to deliver better services to the community. A key goal will be enhancing the government's use of cloud services where appropriate. To achieve this, the default expectation is that 'light' users of ICT services, agencies that have simpler, non-specialised ICT needs, will move to cloud services.[131] 'Heavy' users that have large scale, complex ICT systems will be able to determine whether or not to utilise cloud, but will need to account for their decisions.[132]

Overview of existing regulation

Under the Australian Government's Cloud Computing Policy agencies are required to[133]:

- consider cloud services for new ICT procurements and choose a cloud service where it represents the best value for money and adequate management of risk compared to other available options
- transition public facing websites to public cloud services at appropriate

[130] AGIMO, *Australian Government Cloud Computing Policy*, Version 2, www.finance.gov.au/cloud/, May 2013, p. 4.
[131] Liberal Party of Australia, *The Coalition's Policy for e-Government and the Digital Economy*, www.liberal.org.au/latest-news/2013/09/02/coalition%E2%80%99s-plan-digital-economy-e-government, August 2013, p. 22.
[132] Ibid.
[133] AGIMO, *Australian Government Cloud Computing Policy*, Version 2, www.finance.gov.au/cloud/, May 2013, p. 4.

refreshment points, provided they represent best value for money and are fit for purpose

- establish procedures for sharing information on the use of cloud services throughout government to facilitate continual improvement.

Outsourcing and offshoring

In July 2013, the then Attorney-General, the Hon Mark Dreyfus MP, and Minister Assisting for the Digital Economy, Senator the Hon Kate Lundy, released the Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements (Policy and Risk Management Guidelines).[134] The Policy and Risk Management Guidelines outline a common approach to the storage of unclassified government information on cloud services by government agencies. This approach is based on risk management, and focuses on the confidentiality, availability and integrity of Australian Government information, with a particular emphasis on the protection of Australian citizens' personal information as defined in the *Privacy Act 1988*. The policy reflects the community's expectations that government information will be subject to appropriate protection.

For information of any sort (excluding classified information) that will be handled, stored, transmitted, transported or disposed of in a private, internal or community cloud that is hosted domestically, agencies need only undertake a risk assessment and ensure that arrangements are managed in accordance with the Australian Government Information Security Management Protocol in the Protective Security Policy Framework (PSPF).

For arrangements involving any cloud service hosted offshore or public cloud services hosted domestically, the policy divides unclassified information into three categories:

- Unclassified publicly available information can be stored offshore or in an Australian public cloud with a risk assessment conducted at agency level. Information must be managed in accordance with the Australian Government Information Security Management Protocol.
- Unclassified information that is not publicly available can be stored offshore or in an Australian public cloud with a risk assessment conducted at agency level. The agency head must also document that they have calculated and accepted the associated security risks in accordance with government guidelines.
- All information requiring privacy protections, can only be stored offshore or in an Australian public cloud provided the relevant portfolio Minister agrees

[134] Attorney-General's Department, *Policy and Risk Management Guidelines for the storage and processing of Australian Government information in outsourced and offshore ICT arrangements*, www.protectivesecurity.gov.au/informationsecurity/Pages/Supporting-guidelines-to-information-security-%28including-the-classification-system%29.aspx#guidelines, July 2013.

that sufficient technological and other measures have been implemented to mitigate the risk of unauthorised access. There must also have been consultation with and agreement from the Attorney-General (as the Minister responsible for privacy and the security of government information).

The policy contains a commitment for a review of the policy by the Attorney-General's Department, the Australian Government Information Management Office and the Department of Communications within 12-24 months after implementation.[135] In recognition of the speed of change in the cloud services market, it is expected that the policy will be subject to ongoing reviews.

The Information Security Manual, issued by the Australian Signals Directorate (ASD), sets out the Government's information security management controls.[136] These requirements include that:

- Systems used to store classified information must be located in Australia.[137]
- To store or process classified information in a public cloud service, the handling requirements must have been downgraded.[138]
- Agencies must ensure that service providers seek their approval prior to transferring or allowing access to any government information outside Australia.[139]
- Systems used to store any government information must be accredited to the same minimum standard as the agency's own systems.[140]
- An agency should assess the security risks of using a cloud service to store any government information against ASD's Cloud Computing Security Considerations document.[141]

Ultimately the need to ensure there is competition in the cloud services market must be balanced against the need for appropriate protections, particularly to ensure that government data meets appropriate security and privacy settings. Data held by government is necessarily subject to more stringent rules, including the *Privacy Act 1988*, the *Archives Act 1983* and the *Freedom of Information Act 1982*. See Chapter 3 for more information about the regulation that applies to data protection and privacy.

---

[135] Attorney-General's Department, *Policy and Risk Management Guidelines for the storage and processing of Australian Government information in outsourced and offshore ICT arrangements*, www.protectivesecurity.gov.au/informationsecurity/Pages/Supporting-guidelines-to-information-security-%28including-the-classification-system%29.aspx#guidelines, July 2013, page 18.
[136] Australian Signals Directorate, *Information Security Manual 2014 – Controls Manual*, www.asd.gov.au/infosec/ism/index.htm, 2014.
[137] Ibid, Control 0873, p. 19.
[138] Ibid, Control 1378.
[139] Ibid, Control 1073.
[140] Ibid, Control 0872, p. 20.
[141] Ibid, Control 1210, p. 20.

Similar policies have been put in place internationally. For example, the EU's offshoring and outsourcing laws require personal information to be stored in the customer's country of origin. The International Telecommunications Union, however, has called for the implementation of cloud-aware legal frameworks over policies that restrict the international flow of data.[142]

Commonwealth Procurement Rules

Australian Government financial management is established and supported by a range of legislation including the *Financial Management and Accountability Act 1997* (the FMA Act). The Commonwealth Procurement Rules, made under FMA Act, set out the arrangements for procurement of goods and services by Commonwealth government agencies. The Rules cover the following topics:

- value for money
- encouraging competition
- efficient, effective and ethical procurement
- accountability and transparency in procurement
- procurement risk
- procurement method.

Encouraging competition is a key element of the procurement framework. To achieve this all potential suppliers must 'be treated equitably based on their commercial, legal, technical and financial abilities and not be discriminated against due to their size, degree of foreign affiliation or ownership, location, or the origin of their goods and services'.[143]

Agencies subject to the Commonwealth Procurement Rules must consider these in addition to the Policy and Risk Management Guidelines outlined above in making decisions regarding procurement of cloud services.

Potential triggers

The Policy and Risk Management Guidelines are intended to enhance the checks and balances agencies must apply when seeking to off-shore or outsource the storage and processing of government information, particularly where it contains personal information. Any consideration of the adoption of cloud must carefully consider privacy and security questions. Ultimately, the failure of agencies to properly consider privacy and security could undermine confidence in the Government as a trusted manager of information.

---

[142] ITU, *Trends in Telecommunications Reform 2013*: Transnational aspects of regulation in a networked society, p. 18.

[143] Department of Finance, *Commonwealth Procurement Rules*, www.finance.gov.au/procurement/procurement-policy-and-guidance/commonwealth-procurement-rules/, July 2012, Rule 5.3.

Given the dynamic nature of the cloud services industry, it is likely that there will be a need for ongoing review of the policy. The following factors may be considered as part of a future review process in determining whether the existing policy strikes the appropriate balance between protection of personal information and agency responsibility for decision making.

- **Adequacy of protections:** Inappropriate or unauthorised use of government information by a cloud service provider may indicate further guidance is needed to ensure privacy protections are adequate. A further factor may be public perception about whether the privacy and security controls for government information are appropriate. The extent to which agencies considering cloud services are undertaking comprehensive risk assessments may also be relevant. One stakeholder has noted that, by improving the clarity of its guidance to agencies, the Government can reduce confusion and build confidence to support broader adoption.
- **Level of take up of public and offshore cloud services:** The level of take up of public or offshore cloud services by Australian Government agencies could be considered in reviewing the policy. Cloud service providers may also have insight as to how the adoption of cloud services in the public sector could be enhanced through administrative or cultural changes. This would need to be assessed within the context of other factors that may affect take up, such as risk assessments for individual projects and cultural approaches to storage of information.
- **Impact on Australian cloud services market:** Over the long term, lower levels of take up of public cloud services could impact the level of foreign investment in onshore public clouds (including multi-tenant data centres for the purposes of the policy). A lower demand for these services may act to reduce investment in Australian multi-tenant data centres.

Conclusion

The Australian Government can play an important role in facilitating the use of cloud services in the broader economy through government policies that appropriately balance the protection of data against the benefits offered by cloud services.

Chapter 5 Questions

19. How can government use of cloud services best facilitate take up among consumers?
20. What are the barriers to greater adoption of cloud services within government? How can these barriers be best addressed?
21. What indicators should government consider to determine whether the Government's use of cloud services is inhibiting take up of cloud services?

Chapter 6: Law enforcement access to data in the cloud

Discussion of issues

This chapter discusses access to data stored in the cloud by Australian law enforcement agencies. It also provides an overview of the interception and access regime under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and *Telecommunications Act 1997* (Telecommunications Act).

Government access to data stored in the cloud, particularly foreign government access, has been the subject of much media focus. However, while concerns have been raised about the reach of the *USA PATRIOT Act of 2001*[144], the practical effect of this law appear to be limited. For example, 2012 research indicated that many jurisdictions have processes in place to enable domestic law enforcement agencies to access data held in a cloud service. The research concluded that there is no significant advantage in storing data in one jurisdiction over another from the perspective of government access.[145] All of the 10 countries considered in the research, including Australia, allow access to data held by a cloud service provider through a formal process (such as a warrant or court order).[146] Eight of the 10 also allow cloud providers to voluntarily provide data through other lawful authority from a law enforcement agency. In many jurisdictions law enforcement agencies may also request data without a warrant where the disclosure is reasonably necessary to prevent, detect, investigate, prosecute, or punish violations of law or serious breaches of standards of conduct.[147]

In some jurisdictions extra-judicial mechanisms (such as coercion) may be available to governments to access the systems of a cloud service provider.

Research on terms and conditions in cloud service contracts noted that very few provide for notification to the customer where data is disclosed, possibly because notification may be prohibited by law.[148]

Overview of existing regulation

Access to telecommunications information is covered by the TIA Act and Part 14 of

---

[144] The full title of this act is: the *Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001.*
[145] W Maxwell and C Wolf, *A Global Reality: Governmental Access to Data in the Cloud*, Hogan Lovells White Paper, 23 May 2012, p. 3.
[146] Ibid, p. 13.
[147] Ibid, p. 6.
[148] M Vincent and K Crooks, *Cloud Computing in 2013 – What legal commitments can you expect from your provider?*, Shelston IP Lawyers, 18 February 2013, p. 6.

the Telecommunications Act. These acts aim to protect the privacy of users of telecommunications services in Australia by prohibiting access or interception of communications and telecommunications information except in authorised circumstances. The *Australian Security Intelligence Organisation Act 1979* enables lawful access to information by the Australian Security Intelligence Organisation (ASIO).

Section 5 of the TIA Act sets out a broad definition of 'communication', including a conversation or message or part thereof, including in the form of speech, music or other sounds; data; text; visual images; signals; or in any other form or combination of forms. The TIA Act is intended to be technology-neutral.

The TIA Act includes:

- general prohibitions on the interception of telecommunications[149] and access to stored communications[150]
- systems for issuing warrants to allow interception of telecommunications passing over a telecommunications system[151] and to allow access to stored communications held by carriers and carriage service providers[152]
- an obligation on carriers and carriage service providers to develop, install and maintain the ability to intercept communications on their services[153]
- a system for preserving stored communications held by carriers and carriage service providers[154]
- a system to enable voluntary disclosure or disclosure upon authorisation of telecommunications data (this excludes the contents and substance of a communication) by the 'holder' of that data.[155]

Under the TIA Act, there are eight types of interception warrants allowing real-time access to communications content and a further warrant that enables an agency to access stored communications. There are currently 17 Commonwealth, state and territory law enforcement agencies (plus ASIO) that can access real-time content under a warrant for activities prejudicial to security, or to allow investigation of a 'serious offence'. Serious offences are further defined in the TIA Act, and generally carry a sentence of at least seven years' imprisonment, or are deemed sufficiently serious to justify the use of interception warrants for their investigation. The stored communications warrant allows broader access by criminal law and civil penalty law enforcement agencies, public revenue agencies and other regulatory bodies at the Commonwealth, state and territory level. Such a warrant is available for

[149] Part 2-1 of the TIA Act.
[150] Part 3-1 of the TIA Act.
[151] Parts 2-2 and 2-3 of the TIA Act.
[152] Parts 3-2 and3-3 of the TIA Act.
[153] Section 191 of the TIA Act.
[154] Part 3-1A of the TIA Act.
[155] Chapter 4 of the TIA Act.

investigation of a serious contravention punishable by at least three years imprisonment or 180 penalty units.

Section 313(3) of the Telecommunications Act sets out the requirement for a carrier or carriage service provider to give to officers and authorities of the Commonwealth, a State or Territory 'such help as is reasonably necessary for' the purposes of enforcement of the criminal law or a civil penalty law, enforcement of a criminal law in a foreign jurisdiction, protecting the public revenue or safeguarding national security. Section 313 of the Telecommunications Act also clarifies that a carrier or carriage service provider is not liable in a legal action or other proceeding for damages for providing assistance in good faith under that section or under similar sections contained in the TIA Act.

In addition, the *Australian Security Intelligence Organisation Act 1979* enables ASIO, under warrant, to obtain data held in a particular computer, the target computer, where the information will substantially assist in the collection of intelligence in respect of a matter that is important in relation to security.[156]

The *Cybercrime Act 2001*, *Crimes Act 1914* and *Criminal Code Act 1995* also provide certain enforcement powers relating to computer-based offences. Under the Crimes Act, law enforcement agencies may request electronic documents from a cloud service provider without court approval where there are reasonable grounds to believe they will be relevant to the investigation of a serious terrorism offence.[157]

The extent to which a cloud service provider will be considered a carriage service provider will depend on the specific services provided by the cloud service provider. Discussion about the coverage of cloud service providers is contained in Chapter 2.

The Parliamentary Joint Committee on Intelligence and Security recently completed a review of possible reforms to national security legislation. The Committee considered a package of reforms to the Telecommunications Act, the TIA Act, the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*. The Committee's final report, which was tabled on 24 June 2013, made 43 recommendations, including a comprehensive review of telecommunications interception legislation.[158]

The current regime is based on a single player model, with the assumption that the majority of communications are transmitted over a fixed-line network. While the legislation is technology-neutral in its approach, there is a need to recognise the significant advancements in technology and changes to industry structure and consumer behaviour.

---

[156] W Maxwell and C Wolf, *A Sober Look at National Security Access to Data in the Cloud*, A Hogan Lovells White Paper, 22 May 2013, p. 6.
[157] Ibid.
[158] Parliamentary Joint Committee on Intelligence and Security, Report of the Inquiry into Potential Reforms of Australia's National Security Legislation, www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm, May 2013.

There is some uncertainty about the application of the existing interception regime beyond carriers and carriage service providers. In its discussion paper to the inquiry, the Attorney-General's Department stated:

> The TIA Act only covers C/CSPs, rather than the broad range of current telecommunications industry participants, consistent with the Act's focus on traditional services such as landline telephones. However, the exclusion of providers such as social networking providers and cloud computing providers creates potential vulnerabilities in the interception regime that are capable of being manipulated by criminals.[159]

The Committee formed the view that the existing regime applies more broadly to ancillary service providers:

> …the Committee believes that the TIA Act does, under its existing provisions, include ancillary service providers... The Committee received no evidence on behalf of ancillary service providers which disputed that the TIA Act applied to them.[160]

Setting aside questions of statutory interpretation, the extent to which ancillary service providers that store data outside Australia may be required to comply with warrants and requests for access to information under the TIA Act is likely to be limited by the doctrine of foreign sovereign compulsion.

The Committee's recommendations focus on streamlining and simplifying elements of the interception and access regime. Of particular relevance to cloud service providers is the recommendation to clarify that the TIA Act applies to ancillary providers of telecommunications services accessed within Australia (Recommendation 14).

The Internet Industry Association noted in its submission that:

> Any newly introduced obligations, such as interception and data storage on C/CSPs or extending the obligations to ancillary service providers not currently covered by legislation, should not disadvantage Australian based providers of such services as compared to any overseas competitors operating in Australian markets.[161]

The Committee's views do not represent government policy. The Government is considering its response to the Committee's report.

A Comprehensive inquiry into the TIA Act was referred to the Senate Legal and Constitutional Affairs References Committee on 12 December 2013, with a report to

---

[159] Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats, Discussion Paper*, www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm, July 2012, p. 27.

[160] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm, May 2013, p. 56.

[161] IIA, Submission to Joint Parliamentary Committee on Intelligence and Security, Inquiry into Potential Reforms of National Security Legislation, www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs.htm, August 2012, p. 12.

be completed by 10 June 2014.[162]

Potential triggers

Triggers that may indicate that government access laws are impacting on the Australian cloud services market may include:

- **Lack of certainty among industry:** Cloud service providers may raise concerns about how the interception and access regime applies to cloud services, including the capacity for cloud service providers to participate in cost recovery arrangements.
- **Complaints from consumers:** Consumers may be reluctant to utilise a cloud service if there is a perception that the circumstances in which a cloud service provider can hand over data to a law enforcement agency are unclear.
- **Lower investment in Australian cloud services market:** An interception and access regime that does not clearly set out the circumstances in which access to data in a cloud service is available may lower the level of foreign investment in onshore multi-tenant data centres. If there is a perception that access is broader than in other jurisdictions or that access is available through informal processes this may limit the extent to which it is desirable to store data in Australia.

Conclusion

Clarification of government access laws may provide greater certainty to the cloud services industry about its obligations in this area.

Chapter 6 Questions

22. How are existing government access laws impacting on the cloud services market in Australia?
23. Are there opportunities to lower compliance costs to industry and provide greater certainty and protection to users of cloud services?
24. What measures could Australia undertake internationally to improve trust and confidence?
25. What indicators should government look to, to determine whether government access laws are negatively impacting on the Australian cloud services market?

[162] Visit www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act for more information on the inquiry.

Chapter 7: Regulatory burden

Discussion of issues

This chapter discusses the potential impact of regulatory burden on the Australian cloud services market and the Government's approach to reducing the impact of red tape.

Clear and consistent regulation has benefits to industry and consumers, as well as to the broader economy. These regulatory settings need to provide certainty and transparency for industry, adequate protections for consumers, while also ensuring that they allow innovation and competition within new markets and new delivery platforms, such as cloud. This is likely to encourage more providers to offer cloud services in the Australian market and may further promote Australia as a hub for data centres.

In Australia, a range of regulation may apply to cloud services. Some regulation applies to a specific industry or a section of an industry based on the business model or service offerings provided. Given the broad range of business models and service offerings in the cloud services market, regulatory measures do not currently apply consistently to all cloud service providers. This issue is by no means specific to Australia. As noted in the International Telecommunications Union's Trends in Telecommunication Reform 2013 Report:

> As an initial matter, the regulatory characterization and treatment of cloud computing may itself deter its take-up until regulators clarify the situation. Are cloud services a telecommunications service or an information service; and who should regulate them?[163]

The BSA Global Cloud Computing Scorecard analyses the policy settings that support cloud computing, such as appropriate data protection, adequate security protection, measures to prevent cybercrime, intellectual property rights, policies promoting free trade and underlying infrastructure.[164] Australia ranked second in the 2013 Scorecard, behind Japan and ahead of the US.

Notwithstanding these findings, there may be areas in which current regulatory settings may be unclear, impose inconsistent obligations or create significant differences in the regulatory settings between jurisdictions that have an impact on cloud service providers.

Deregulation

Cloud computing may be subject to a broad range of Commonwealth legislation, in addition to state or territory legislation and industry standards, which may lead to uncertainty or inconsistency for industry. While appropriate regulatory settings can play an important role in ensuring consumer confidence in cloud services, over-regulation can be a drain on productivity, can needlessly increase compliance costs,

[163] ITU, *Trends in Telecommunications Reform 2013: Transnational aspects of regulation in a networked society*, p. 15.
[164] BSA Software Alliance, *Global Cloud Computing Scorecard*, cloudscorecard.bsa.org/2013/, 2013.

raise barriers to entry, reduce competition, and ultimately harms consumers through higher prices and less choice.

The Government has recognised the burden unnecessary red and green tape places on business, and ultimately, consumers.[165] The Government has signalled that it will seek to introduce a $1 billion per year target for red tape reduction. As part of this process there will be a review of existing regulatory arrangements with a view to identifying areas in which regulation is ineffective, out of date, imposes significant costs on industry that do not outweigh the benefits, or creates uncertainty over obligations.

There will also be a focus on the removal of regulatory burden that restricts the flow of trade and has the potential to redirect international investment to other jurisdictions with a more favourable competitive environment and regulatory settings.[166]

Policy framework

Regulation should not be a first response when issues are identified[167], particularly at a relatively early stage in take up of a new service type. The preference is instead to look to ways for the Government to work with industry to address potential issues, such as through consumer education initiatives. However, there remain instances in which government intervention may be warranted.

According to the Office of Best Practice Regulation (OBPR), government intervention may be appropriate where a policy problem has arisen as a result of market failure, regulatory failure or unacceptable hazard or risk.[168] While market failure is often a key indicator that intervention may be needed, government intervention does not rely solely on its presence, as there are a range of legitimate rationales for introducing regulation, such as social policy outcomes.[169]

The delivery of social policy outcomes is relevant in a cloud context. Goals such as protecting consumers in contractual arrangements and in the use of and access to personal information have strong social equity aims. A key objective for government regulation is an overall improvement in community welfare, balanced against the impact it may have on competition, productivity and economic growth. In practice a coherent and responsive regulatory approach will be informed by both evidence of market failure and promotion of social policy outcomes.

Further discussion on market failure and an overview of the general regulatory options available to government are provided in **Attachment A**.

---

[165] Liberal Party of Australia, *Coalition's Policy to Boost Productivity and Reduce Regulation*, www.liberal.org.au/latest-news/2013/07/08/coalitions-policy-boost-productivity-and-reduce-regulation, August 2013.
[166] Ibid, p. 22-23.
[167] Ibid, p. 13.
[168] Department of Prime Minister and Cabinet, *The Australian Government Guide to Regulation*, www.cuttingredtape.gov.au, March 2014, p. 22.
[169] Ibid.

Overview of existing regulation

Areas of regulation that may impact on cloud services include copyright and competition, consumer protection, privacy, cybersecurity and government access. Extensive laws applying to corporations, and taxation and electronic transactions are also applicable to cloud services. In addition, there are currently approximately 450 pieces of legislation that deal with record keeping requirements for different purposes, such as taxation, workplace relations and corporations law and may impact on users of cloud services.[170] Apart from government regulation, there may be industry-based standards (including technical standards) that apply to cloud services, at the national, regional or international level.

There are areas in which differences between regulatory settings in Australia and overseas may impact on the ability of Australian cloud services to compete globally, as well as the desire of international cloud service providers to provide services to the Australian market. This can create difficulties for global cloud service providers that need to comply with potentially inconsistent regimes.

Regulation can be complex to interpret, and can apply in unexpected ways to novel services such as cloud computing. Given the speed with which new and emerging technologies have evolved, there may also be areas in which Australian laws have failed to adequately address the issues raised by these technologies. This can create confusion and uncertainty among both providers and users of cloud services. In fact, one major supplier of cloud services has indicated that the largest constraint in the cloud services market is one of a lack of regulatory clarity, particularly in relation to the public and financial sectors. It has been suggested that one focus of government should be to improve the ability of organisations operating in highly regulated markets to adopt cloud services.

In 2013, the Australian Computing Society explored the introduction of a voluntary Cloud Computing Protocol that would set guidelines around the information provided to consumers of cloud services. Consultation with industry stakeholders emphasised that further regulation at a relatively early stage of a new technology could have detrimental effects on competition in the Australian cloud services market.[171]

Potential triggers

Over-regulation may have a detrimental impact on the Australian economy. Triggers that may indicate that there is excessive or complex regulation impacting on the Australian cloud services market include:

---

[170] A Wong, *Understanding the legal framework of moving to cloud computing*, Speech to CeBIT, http://www.slideshare.net/CeBITAustralia/cloud-computing-conference-2011-anthony-wong-acs, 31 May 2011.

[171] ACS, Cloud Computing Consumer Protocol - Submissions, www.acs.org.au/information-resources/public-policy/2013-australian-cloud-protocol/2013-australian-cloud-protocol-submissions, 2013.

- **Lack of certainty or understanding of regulatory settings among cloud service providers:** Cloud service providers will be in the best position to identify and advise government where regulation leads to unnecessary complexity or may have the effect of stifling innovation. A market that lacks diversity of offerings may indicate that regulation may be stifling innovation.
- **Significant differences in regulation between international jurisdictions makes it difficult for Australian cloud service providers to compete globally:** Cloud service providers may raise concerns about differences in regulation between jurisdictions. The development of customer local standards could reduce the competition in the Australian cloud services market. The development of standards particular to one geographical or political region could decrease the ability of multinational vendors to provide their services in those regions.
- **There is difficulty effectively addressing complaints:** Complaints data from regulators, dispute resolution schemes (such as the Telecommunications Industry Ombudsman) and disputes taken to court, could be an indicator of overly complex or unclear rules. Engagement between regulators and industry may also be indicative of concerns by industry about the application of certain regulation. For example, parties may be less likely to pursue a dispute if there is a lack of clarity over which party has the stronger legal claim. Industry may also be more likely to seek guidance from regulators where the application of law is unclear.
- **Significant price differentials and difference of service offerings between jurisdictions:** Higher prices and less choice for cloud products could be an indicator that the price of doing business in Australia is higher than in other jurisdictions. Further, significant differences in the terms and conditions for service offerings between jurisdictions may be indicative of broader problems in the Australian market. Over-regulation could be a contributing factor, although there are likely to be other factors (such as exchange rate differences) that offer better explanations.

Conclusion

Identification and removal of regulatory burdens is a key objective of the Government's agenda. Clearer and more consistent regulation would benefit consumers and industry alike and help make Australia a more competitive jurisdiction.

Chapter 7 Questions

26. What impact is red tape having on the cloud services market in Australia?
27. How do the compliance obligations imposed by Australian law compare to other jurisdictions?
28. How well is the current regulatory environment understood by the market?
29. What opportunities exist to reduce compliance costs for cloud service providers and users of cloud services?
30. What non-regulatory actions could government undertake to encourage the take up of cloud services? Should there be a focus on highly regulated markets?
31. What indicators should government consider to determine whether there is over-regulation in the cloud service market?

Attachment A: Market failure and potential forms of government intervention

Market failure

This attachment provides more information about the concept of market failure as a trigger for government intervention and an overview of the main types of intervention available to government. As noted in Chapter 7 of this stock take, market failure is one indicator that there may be a need for intervention, with social policy outcomes another key indicator. This attachment draws on the Australian Government Guide to Regulation.

A starting point for determining whether government intervention is appropriate is identifying the underlying problem that is the cause of the market failure or that is indicative of future market failure. Relevant considerations include the degree of the failure, its impact and whether the proposed intervention would produce an overall improvement in community welfare.[172] Market failure occurs where markets do not produce economically efficient outcomes. Government intervention can, to a certain extent, correct market failures and improve community welfare as long as the benefits of the intervention outweigh the costs.

Economic efficiency

In economic theory, economic efficiency refers to the allocation of resources to maximise the production of goods and services. It is distinct from notions of equity or fairness, and describes a hypothetical market where resources are allocated so that no one can be made better off without making someone worse off.

All intervention in markets, whether by government or other entities, has risk and costs associated with it. In some circumstances, intervention in a market may not correct the identified market failure or may introduce a new problem. For example, even minimal intervention by government, such as an education initiative, carries a cost to tax payers and may change purchasing preferences to favour less economically efficient outcomes.

It is worth noting that all markets are inefficient to some extent. Further complicating matters may include:

- Parts of markets can be considered distinct for the purposes of intervention, either because they are geographically distinct, or because they sell significantly different products (such as commercial versus residential property insurance), or they service significantly different customers.

[172] Department of Prime Minister and Cabinet, *The Australian Government Guide to Regulation*, www.cuttingredtape.gov.au, March 2014, p. 18.

- Markets are generally dynamic. Changes in demand or supply can impact market structures, or vice versa. Changes in the consumption of complementary goods or competing goods can also change markets. For example, an increase in the consumption of smartphones will likely lead to an increase in the consumption of mobile phone applications.

There are four categories of market failure identified by OBPR[173]: monopoly and abuse of power; information asymmetry; externalities and public goods.

Monopoly and abuse of power

This occurs where there is restricted competition within a marketplace which may affect the entry of new participants or where there is market domination by one or more participants.[174] Market power occurs when a firm or individual is able to raise the price of its good or service over the marginal cost while still making a profit.[175]

> Example: Raising switching costs
>
> This may occur where there are technical or legal barriers preventing customers switching to new providers. Referred to as **vendor lock-in**, this may allow a firm to increase prices or lower the quality of services (for example, by not dealing effectively with consumer complaints) without customers being able to switch to new providers efficiently (or without significant cost).

Information Asymmetry

Information Asymmetry may occur where one party to a transaction has significantly more information than another, allowing them to make more efficient decisions.[176]

The ACMA's Reconnecting the Customer Inquiry from September 2011 identified asymmetry of information as a key concern in the telecommunications industry, noting that consumers have limited information about service quality, complaint handling processes and pricing.[177] Further, this asymmetry of information meant that consumers have trouble assessing the exact terms of services and the post-sale customer service of different providers to assist them in making decisions about goods and service. The inquiry recommended a range of improvements to enhance consumer protections.

---

[173] Department of Prime Minister and Cabinet, *The Australian Government Guide to Regulation*, www.cuttingredtape.gov.au, March 2014, pp. 22-23.
[174] Ibid.
[175] Ibid. Market power can also occur where a firm can demand a price less than the efficient economic cost of a good or service – known as a monopsony.
[176] Ibid.
[177] ACMA, *Reconnecting the Customer: Final public enquiry report*, September 2011.

Example: Moral hazard

A moral hazard is where a business has different incentives to its consumer and therefore treats risk differently. This may occur where a cloud service provider does not have clear regulations relating to privacy and does not have full knowledge of the type of information being stored on its service. As a result, it may not have sufficient incentives to keep personal information on its service secure.

Externalities

Externalities are costs and benefits imposed on parties that are not involved in a transaction.[178] There are both positive externalities and negative externalities. The presence of externalities alone does not indicate that intervention is necessary, the size and nature of the externality must be considered as well as the ability to address it at low cost through intervention.[179]

Example: Copyright breach

A customer may use a cloud service to distribute copyright infringing material, which could impact on the value of the legitimate right holder's intellectual property rights.

Public goods

Public goods are goods that are non-rivalrous and non-excludable.[180] This means one person's consumption does not affect the ability of others to consume the good or service and it is difficult both to exclude people from consuming the good or service and to charge consumers for their consumption. Public goods do not generally relate to cloud services, and so are not considered further for the purpose of this analysis.

Behavioural market failure

Behavioural economics relates to the decisions that individuals make, or are perceived to make, that are against their own best interests. It may have relevance to the design of regulations that are intended to result in a change in consumer behaviour. To determine a behavioural market failure, evidence needs to show that consumers could have been better off if they made a different choice.

Options for intervention

As noted above, this stock take seeks to identify the conditions and triggers that may

[178] Department of Prime Minister and Cabinet, *The Australian Government Guide to Regulation*, www.cuttingredtape.gov.au, March 2014, p. 23.
[179] Ibid.
[180] Ibid, p. 24.

warrant government intervention in the cloud services market. Potential triggers are discussed for each chapter. It is critically important that government look to ensure that identified triggers are appropriate and that there is strong evidence of market failure before considering whether to intervene in any market.

This stock take does not set out specific government intervention that would be considered if market failure was evidenced or if the Government was seeking to achieve a specific social equity objective. However, it is worth noting generally that government has a range of options for intervention open to it, and that the least intrusive option with the least compliance cost and chance for unintended side effects should be preferred if intervention is warranted.

This section outlines, at a high level, potential options for government intervention and their potential application in a cloud computing context.

Education initiatives: Consumer education can be an effective approach to overcome information asymmetry and to promote informed consumer decisions. Education initiatives can be funded by taxpayers or can be funded collectively by industry or other private sector groups.

Education initiatives that target information at cloud service providers rather than consumers may also be an effective approach to address consumer concerns by providing guidance on the application of existing regulation. In a similar vein, a statement by a regulator about acceptable behaviour may assist industry in meeting its regulatory obligations.

Key advantages of education initiatives are that they can be cost effective (that is, there is unlikely to be a significant whole of economy cost) and are unlikely to have unintended side effects.

In relation to cloud computing, the Government already produces a range of material to help consumers make informed decisions about cloud. This includes information provided publicly (such as information available through the digitalbuisness.gov.au and business.gov.au websites) and more targeted information provided through existing government programs (such as the Small Business Advisory Service and the Enterprise Connect program). The Government is also working on the publication of guidance on the application of privacy legislation to cloud computing.

Self-regulation: The Government encourages the use of self-regulatory measures where appropriate as an alternative to regulation. Under self-regulation the relevant industry establishes standards or codes of conduct to address certain behaviour. There must be an incentive for industry to comply with the standards or codes to ensure self-regulation is effective as enforcement of the rules is generally handled within the industry or through a body set up by industry.[181] Examples of pure self-regulation, without a legal safety net (such as a regulator empowered to enforce

[181]ACMA, *Optimal conditions for effective self- and co-regulatory arrangements*, Occasional Paper, www.acma.gov.au/theACMA/optimal-conditions-for-effective-self-and-coregulatory-arrangements, September 2011, p. 4.

codes) are rare in Australia.[182] Self-regulation can have lower compliance costs, because the relevant industry is involved in the rule development process. Consequently, rules decided can be very well tailored to the particular industry.

Best practice regulation guidelines indicate that self-regulation is most appropriate where the problem is low-risk or of low significance or the market is likely to be able to address the problem itself.[183]

Cloud services are broad and are not currently represented by a single industry body, although there are industry bodies that have an interest in cloud services. The ACMA has noted that the small number of data centres in Australia and the diverse participants within the market may have prevented the development of an industry code.[184] Despite this, the ACMA notes that the cloud services market currently has the markers of a successful self-regulatory approach: the presence of a competitive market, with few barriers to entry and a rapidly changing environment.[185]

Co and Quasi-Regulation: Co-regulation combines a mixture of industry-developed regulation, for example through codes and standards of practice, with government enforcement through legislation. While the industry may play some role in the enforcement of such a scheme, legislative backing enables the relevant regulator to take action where appropriate. Co-regulation is more common in Australia than self-regulation, for example, the regulation of carriage service providers under the Telecommunications Industry Ombudsman (TIO) scheme.[186] The TIO is a non-government body, funded by industry, but backed by legislative powers and the membership of the scheme is mandated by legislation.

The OECD has identified a range of advantages to self-regulatory and co-regulatory approaches, when used in appropriate circumstances, including:

- increased flexibility and adaptability
- the potential for reduced compliance and administrative costs
- the use of industry knowledge and expertise to address specific issues
- time and cost-effective complaint handling processes.

As is the case with the issues identified with self-regulatory approaches, a

---

[182] ACMA, *Optimal conditions for effective self- and co-regulatory arrangements*, Occasional Paper, www.acma.gov.au/theACMA/optimal-conditions-for-effective-self-and-coregulatory-arrangements, September 2011, p. 4.
[183] Department of Prime Minister and Cabinet, *The Australian Government Guide to Regulation*, www.cuttingredtape.gov.au, March 2014, p. 28.
[184] ACMA, *The Cloud: services, computing and digital data – Emerging issues in media and communications*, Occasional Paper 3, www.acma.gov.au/Citizen/Stay-protected/My-online-world/Staying-safe-online/coherent-regulation-best-for-cloud-services, June 2013, p. 20.
[185] Ibid and ACMA, *Optimal conditions for effective self- and co-regulatory arrangements*, Occasional Paper, www.acma.gov.au/theACMA/optimal-conditions-for-effective-self-and-coregulatory-arrangements, September 2011, p. 12.
[186] Visit www.TIO.com.au for more information about the TIO.

co-regulatory approach must provide clear guidance to industry about appropriate practices while ensuring an effective complaint handling enforcement regime. The involvement of the regulator in approving a code or standard may also ensure that the interests of industry are effectively balanced against those of consumers.

Quasi-regulation, on the other hand, includes measures such as industry accreditation schemes, guidance notes and codes of practice that may be developed with involvement by government and are intended to encourage compliance but are not government regulation.

Similar issues to self-regulation arise with co and quasi regulation. It is worth noting that while co and quasi regulation can have lower regulatory burden than government regulation, there can still be significant compliance costs which should be considered by decision makers.

Government regulation: The most commonly used form of regulation is government regulation through primary or subordinate legislation.[187]

It is government policy that regulation is a last resort. Regulatory guidelines indicate that government regulation may be most appropriate in situations in which the problem is of high-risk or public significance.[188]

As discussed throughout the stock take, there are a range of existing regulatory measures that may apply to certain aspects of or certain providers of cloud services.

The ACMA, in its occasional paper on cloud computing, noted the importance of a single coherent framework of regulation for cloud services to replace the existing complex mix of regulatory arrangements.[189] The ACMA raised concerns that the current regulatory settings for telecommunications lead to differential treatment of like services by limiting regulation to traditional industry participants or delivery platforms.[190] This may lead to the risk of a lack of adequate consumer protections or a lack of certainty for industry and consumers. An example of this is streaming and sharing of content via a cloud service, which may not be subject to the same classification rules for television and radio.[191]

However, the ACMA has also recognised that '…strategies other than traditional regulation may offer a more efficient way of solving digital citizen problems, particularly where industry suppliers are outside national jurisdictions'.[192] It has also proposed that '[a] different mix of strategies, working with a range of participants

---

[187] Department of Prime Minister and Cabinet, *The Australian Government Guide to Regulation*, www.cuttingredtape.gov.au, March 2014, p. 29.
[188] Ibid.
[189] ACMA, *The Cloud: services, computing and digital data – Emerging issues in media and communications*, Occasional Paper 3, www.acma.gov.au/Citizen/Stay-protected/My-online-world/Staying-safe-online/coherent-regulation-best-for-cloud-services, June 2013, p. 12.
[190] Ibid, pp. 13-14.
[191] Ibid, p. 14.
[192] ACMA, *Connected citizens – A regulatory strategy for the networked society and information economy*, www.acma.gov.au/theACMA/About/The-ACMA-story/Connected-regulation/regulating-for-connected-citizens, June 2013, p 20.

and recognising shared responsibilities, may be needed in this more dynamic and highly connected network environment'.[193]

Generally, regulation should be the option of last resort. While a minimal degree of regulation is required, over-regulation can have significant hidden costs to business that are passed on to consumers. The Government has identified that public policy makers should utilise the Regulation Impact Statement process to quantify the whole of economy costs and benefits of proposed regulation, and alternatives to regulations, before deciding to proceed with legislation.

[193] Ibid, p 27.

Attachment B: Relevant Commonwealth legislation

This attachment sets out the legislation referred to within this stock take that may be relevant to cloud services.

- *Archives Act 1983*
- *Australian Security Intelligence Organisation Act 1979*
- *Broadcasting Services Act 1992*
- *Competition and Consumer Act 2010.* The Australian Consumer Law (ACL) is contained in Schedule 2 of the Competition and Consumer Act 2010
- *Copyright Act 1968*
- *Corporations Act 2001*
- *Crimes Act 1914*
- *Criminal Code Act 1995*
- *Cybercrime Act 2001*
- *Cybercrime Legislation Amendment Act 2012*
- *Financial Management and Accountability Act 1997*
- *Freedom of Information Act 1982*
- *Intelligence Services Act 2001*
- *Personally Controlled Electronic Health Records Act 2012*
- *Privacy Act 1988*
- *Telecommunications Act 1997*
- *Telecommunications (Consumer Protection and Service Standards) Act 1999*
- *Telecommunications (Interception and Access) Act 1979*

Attachment C: Relevant state and territory legislation

This attachment provides an overview of the state and territory legislation that may be applicable to cloud computing, based on the issues outlined in this stock take. Information has been provided by relevant state and territory departments.

Competition and copyright

State and territory legislation mirrors the Australian Consumer Law in terms of certain types of anti-competitive conduct directed at consumers, such as misleading and deceptive conduct or unconscionable conduct, see below under Contractual arrangements and consumer protection. Other types of conduct, such as misuse of market power, are covered by the Commonwealth *Competition and Consumer Act 2010*.

The only state that has enacted copyright legislation is New South Wales (NSW). The *Copyright Act 1879* deals only with the use of certain works by libraries, as the *Copyright Act 1968* 'covers the field' on copyright.

'Cover the field'

If there is inconsistency between a Commonwealth law and a state or territory law, the Commonwealth law prevails under section 109 of the Constitution. Commonwealth legislation can also 'cover the field' – where there is an intention for the Commonwealth law to be all the law on a particular topic.

Contractual arrangements and consumer protection

The Australian Consumer Law (ACL) commenced on 1 January 2011, replacing a range of state and territory fair trading legislation. New legislation was introduced in each state and territory to enable consistent application of the ACL as a national application law. Individual complaints are generally investigated by the relevant state or territory fair trading association. The table below provides a list of the legislation that applies the ACL in each state and territory.

Note that there are some other consumer trading laws that still apply in each state and territory and may have application beyond the ACL. For example, in NSW the *Consumer Claims Act 1998* provides a dispute resolution process for consumers of goods and services through the Consumer, Trader and Tenancy Tribunal.

Australian Capital Territory	*Fair Trading (Australian Consumer Law) Act 1992* (ACT)
New South Wales	*Fair Trading Act 1987* (NSW)
Northern Territory	*Consumer Affairs and Fair Trading Act* (NT)
Queensland	*Fair Trading Act 1989* (Qld)

South Australia	*Fair Trading Act 1987* (SA)
Tasmania	*Australian Consumer Law (Tasmania) Act 2010* (Tas)
Victoria	*Fair Trading Act 1999* (Vic)
Western Australia	*Fair Trading Act 2010* (WA)

Data protection and privacy

Most of the states and territories have privacy legislation that is generally consistent with the Commonwealth *Privacy Act 1988* (Privacy Act). States and territories also have separate legislation dealing with privacy obligations within the health sector.

State and territory privacy frameworks impose obligations on state and territory government agencies and, in some cases, private sector organisations with whom they contract. The Privacy Act sets out obligations on Commonwealth agencies and private sector organisations that come within the coverage of the legislation.

Amendments made to the Privacy Act in 2012 (which are due to come into practice in March 2014) went some way to standardise provisions across Commonwealth and state and territory legislation. These include the definition of personal information and the key concepts in the legislation.

In addition to privacy legislation, there are record keeping requirements at the state or territory level that apply to certain types of information (for example, corporations or workplace relations) or specific industries (for example, the legal profession, financial services or the construction industry), which may be relevant for consumers of cloud services to consider when considering the impact of moving their data to the cloud.

Australian Capital Territory	*Privacy Act 1988* (Commonwealth)
New South Wales	*Privacy and Personal Information Protection Act 1988* (NSW)
Northern Territory	*Information Act 2002* (NT)
Queensland	*Information Privacy Act 2009* (QLD)
South Australia	South Australia has an administrative instruction requiring agencies to meet a set of Information Privacy Principles, but currently has no privacy legislation
Tasmania	*Personal Information and Protection Act 2004* (Tas)
Victoria	*Information Privacy Act 2000* (Vic)
Western Australia	There is no current privacy legislation in

	Western Australia. Rather, confidentiality provisions cover government agencies and the *Freedom of Information Act 1992* (WA) provides some privacy principles

Cybersecurity

Each state and territory has enacted legislation introducing similar computer-based offences to those contained in Part 10.7 of the Commonwealth *Criminal Code Act 1995*. The states and territories have jurisdiction over cybercrimes that affect individuals, businesses and government systems in their own jurisdictions. The Commonwealth has responsibility for cybercrimes that target critical infrastructure, systems of national interest and Commonwealth Government systems.[194]

Australian Capital Territory	*Criminal Code 2002* (ACT)
New South Wales	*Crimes Amendment (Computer Offences) Act 2001* (NSW)
Northern Territory	*Criminal Code Act* (NT)
Queensland	*Criminal Code Act 1899* (Qld)
South Australia	*Criminal Code Consolidation Act 1935* (SA)
Tasmania	*Criminal Code Act 1924* (Tas)
Victoria	*Crimes Act 1958* (Vic)
Western Australia	*Criminal Code Act Compilation Act 2013* (WA)

Government use of cloud computing

Many state and territory jurisdictions have requirements around the storage of government information. These may include privacy legislation and record keeping legislation, as well as a range of guidelines and other policies. Each state and territory also has legislation equivalent to the Commonwealth *Freedom of Information Act 1982*, which establishes a regime for access to information held by government and the Commonwealth *Electronic Transactions Act 1999*, which deals with record keeping requirements for electronic records.

Some jurisdictions have also considered the arrangements for storage of government information outside the jurisdiction. For example, the NSW government

[194] The Protocol for Law Enforcement Agencies on Cybercrime Investigations introduced a coordinated approach to dealing with cybercrime across the Commonwealth and state and territory law enforcement agencies. It was endorsed at the Australia and New Zealand Police and Emergency Management Ministerial Meeting on 29 July 2011.

allows the transfer of records out of NSW for storage with or maintenance by service providers based outside of the state[195], which provides for the storage of government information outside of NSW but within Australia, following a risk assessment and provided that records continue to be managed in accordance with relevant laws.

Australian Capital Territory	*Territory Records Act 2002* (ACT)
New South Wales	*State Records Act 1998* (NSW)
Northern Territory	*Information Act 2002* (NT)
Queensland	*Public Records Act 2002* (Qld)
South Australia	*State Records Act 1997* (SA)
Tasmania	*Archives Act 1983* (Tas)
Victoria	*Public Records Act 1973* (Vic)
Western Australia	*State Records Act 2000* (WA)

Law enforcement access to data in the cloud

The Commonwealth *Telecommunications (Interception and Access) Act 1979* sets up a comprehensive national scheme for the lawful interception of telecommunications by Commonwealth, state and territory law enforcement agencies. Each state and territory has complementary legislation to ensure that state and territory law enforcement agencies are subject to the same record keeping, reporting and inspection obligations as those imposed under the Commonwealth legislation.

Australian Capital Territory	*Telecommunications (Interception and Access) Act 1979*
New South Wales	*Telecommunications (Interception and Access) (New South Wales) Act 1987* (NSW)
Northern Territory	*Telecommunications (Interception) Northern Territory Act* (NT)
Queensland	*Telecommunications Interception Act 2009* (Qld)
South Australia	*Telecommunications (Interception) Act 2012* (SA)

[195] Visit www.records.nsw.gov.au/recordkeeping/government-recordkeeping-manual/rules/general-retention-and-disposal-authorities/general-authority-for-transferring-records-out-of-nsw-for-storage-with-or-maintenance-by-service-providers-based-outside-of-the-state-ga-35 for more information.

Tasmania	*Telecommunications (Interception) Tasmania Act 1999* (Tas)
Victoria	*Telecommunications (Interception) (State Provisions) Act 1988* (Vic)
Western Australia	*Telecommunications (Interception and Access) Western Australia Act 1996* (WA)

Attachment D: International approaches to regulation of cloud services

International regulation on cloud computing is an emerging area. This attachment gives an overview of some of the regulatory approaches to cloud computing taken by other countries, as well as broader international frameworks on key issues such as privacy, cybersecurity and copyright.

The European Union (EU) introduced the Digital Agenda Strategy, for 'unleashing the potential of cloud computing in Europe' in September 2012.[196] The strategy includes:

- reducing the technical standards that currently apply to cloud to achieve interoperability, data portability and reversibility for users of cloud services
- supporting certification schemes across the EU to increase the trustworthiness of cloud providers
- developing a model 'safe and fair' contract terms for cloud contracts
- introducing a European Cloud Partnership between industry and EU member states to provide cost-effective and better quality services to government, while assisting in the development of the EU cloud services market.

Compared to the EU's focus on regulatory frameworks, the United Kingdom (UK) and United States (US) governments have mostly concentrated efforts on enhancing cloud use by government, rather than on economy-wide cloud frameworks or regulation. This is reflected in the fact that both countries have cloud first policies and cloud strategies for government ICT[197], but have not published economy-wide cloud policies. Government ICT procurement is seen as a way to encourage innovation in the cloud sector, while enhancing consumer choice.

Singapore has implemented a range of policy initiatives to enhance its reputation as a stable and trusted business environment. For example, it formed a 'cloud computing standards coordinating task force' as part of the Singapore IT Standards Committee, to develop guidelines on cloud security and service levels, including a checklist for cloud users to consider when subscribing to public cloud services.[198]

---

[196] EU, *Digital Agenda: New strategy to drive European business and government productivity via cloud computing* (press release), europa.eu/rapid/press-release_IP-12-1025_en.htm, Brussels, 27 September 2012.

[197] US Government, *Federal Cloud Computing Strategy*, www.whitehouse.gov/sites/.../federal-cloud-computing-strategy.pdf, February 2011, and
UK Government, *Government Cloud Strategy*, www.gov.uk/government/.../government-cloud-strategy_0.pdf, March 2011.

[198] Singapore Government, Infocomm Development Authority, www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&cad=rja&ved=0CEsQFjAA&url=http%3A%2F%2Fwww.ngp.org.sg%2Fdocuments%2FCloud_Computing_in_Singapore_2nd_Edition.pdf&ei=vYJkUpfxDqySiAeIq4CADQ&usg=AFQjCNE1AuXj2fTagRIu_RBGOigWudRBAg&bvm=bv.55139894,d.aGc.

Privacy and data protection

International privacy guidelines

In the area of privacy, best practice guidance on data protection is included in the Organisation for Economic Cooperation and Development (OECD) Guidelines on Privacy and the Asia-Pacific Economic Cooperative (APEC) Privacy Framework.

The OECD Guidelines on Privacy, first developed in 1980, set out high-level principles for the handling of personal information that are designed to encourage consistent laws across member countries.[199] The Guidelines are reflected in privacy and data protection laws internationally and focus on the rights of the individual. The Guidelines were updated in 2013.

The principles in the Guidelines are:

- collection limitation
- data quality
- purpose specification
- use limitation
- security safeguards
- openness
- individual participation
- accountability.

The privacy principles in the *Privacy Act 1988* are based explicitly on the OECD Guidelines on Privacy, with the exception of the accountability principle, which does not correspond to a specific privacy principle but is a component of the data breach provisions in the Act. Amendments to the Privacy Act, due to commence in March 2014, will move from an adequacy approach to cross-border disclosure of information to an accountability approach, consistent with the OECD Guidelines (and APEC Privacy Framework). Under this new approach, where an entity bound by the Act discloses personal information to an overseas recipient that is not bound by the Act and the recipient breaches a privacy principle, the act is taken to have been done by the entity bound by the Act and they would be held accountable for the breach (section 16C).

The APEC Privacy Framework was endorsed by APEC Ministers in 2004 and includes nine principles, many of which overlap with the OECD Guidelines.[200] The Framework focuses on actual and potential harm resulting from the disclosure of personal information and the responsibilities of organisations that collect data. The Framework is intended to provide businesses in the Asia-Pacific region with guidance

[199] Visit oecdprivacy.org/ for more information.
[200] Visit publications.apec.org/publication-detail.php?pub_id=390 for more information.

on how they should appropriately manage personal information. Unlike the OECD Guidelines on Privacy, the Framework is not endorsed by law. Despite this, the ALRC sees the APEC Privacy Framework as an important opportunity to develop a balanced approach in the Asia-Pacific region that is not as reliant on the private sector as the US regime, nor as bureaucratic as the European regime.[201]

There are also other international and regional instruments including various EU directives and Council of Europe Conventions which might have implications for cloud services providers in those jurisdictions.

There has been some work to create an international privacy standard. In 2009, members of the International Conference of Data Protection and Privacy Commissioners adopted a 'Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data', also known as the Madrid Resolution.[202] Principles include fairness, accountability, data quality and openness. The Resolution has been adopted in 50 countries, including Australia, although it is noted that the US is not a signatory.

Approaches in other jurisdictions

The US takes a sectoral approach to privacy protections, combining a mixture of state, federal and sector-specific legislation, as well as industry self-regulation.[203] Particular focus is given to certain industries that deal heavily in personal information, such as health and financial services. The US Federal Trade Commission (FTC) is active in enforcing privacy breaches and can seek fines, in addition to changes to privacy practices and systems audits. The FTC has the power to take action on breaches of the Federal Trade Commission Act of 1914 and 33 other laws that provide enforcement powers in relation to the protection of consumers' privacy.[204] In addition, the FTC has the power to issue industry-wide regulations.

In addition to statutory protections, the US provides a tort for invasions of privacy. Currently, there is no such tort in Australia, however, the Australian Law Reform Commission (ALRC) is currently undertaking a review into the introduction of a statutory tort that would enable citizens to take legal action for serious breaches of privacy.[205]

Other countries that have comprehensive data privacy frameworks include India,

---

[201] ALRC, For Your Information: Australian Privacy Law and Practice, Vol. 1 Executive Summary, www.alrc.gov.au/publications/Executive%20Summary/key-recommendations, 2008.
[202] International Standards of the Protection of Personal Data and Privacy: The Madrid Resolution, www.gov.im/lib/docs/odps//madridresolutionnov09.pdf, 2009.
[203] R Berry and M Reisman, 'Policy Challenges of Cross-Border Cloud Computing', United States International Trade Commission, *Journal of International Commerce and Economics*, May 2012, p. 13.
[204] Visit www.ftc.gov/about-ftc/what-we-do/enforcement-authority and www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises for more information on the FTC's enforcement action.
[205] ALRC, Serious invasions of privacy in the digital era inquiry, discussion paper 80, www.alrc.gov.au/inquiries/invasions-privacy, 31 March 2014.

Japan, Malaysia, South Korea and Taiwan.[206]

Perhaps the most comprehensive privacy regime is in the EU. The EU Data Protection Directive sets standards for the management of personal information within the EU that must be adopted within the privacy laws in member states.[207] The Data Protection Directive specifies minimum measures to be implemented, leaving member countries the option of putting stricter requirements in place.

The directive is currently under review, with a view to introducing a single uniform directive that would apply to 27 member countries from 2014. The revised directive, commonly known as the General Data Protection Regulation[208], seeks to impose higher standards for transfers of data outside of the EU, extending the scope of EU laws to all companies offering goods or services in the EU or monitoring the behaviour of EU residents online. This would mean that any cloud providers with EU customers, which could include some Australian cloud providers, would need to adhere to EU obligations. Cloud providers may apply these obligations to all data they handle, where they provide a higher standard of protection, so the directive could potentially set the international data privacy standard.

Further changes include[209]:

- standards around data portability that would enable EU residents to move data between systems or providers on request
- standards on the right to be forgotten that would require deletion of personal information when consent is withdrawn or when the information is no longer needed
- the requirement for consent to be explicit
- notification standards requiring the inclusion of contact information for both the data processor and data controller and information about how long data will be retained
- a data breach notification scheme which will require notification to the relevant privacy authority and affected individuals within 24 hours of a data breach
- strengthening the penalties and remedies available for breaches of privacy, as well as the powers of national privacy authorities
- individuals will also have the right to refer a privacy breach to the privacy authority in their home country for investigation.

---

[206] R Berry and M Reisman, 'Policy Challenges of Cross-Border Cloud Computing', United States International Trade Commission, *Journal of International Commerce and Economics*, May 2012, p. 13.
[207] Ibid, p. 11.
[208] The full title is the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[209] European Union, Fact *Sheet: Why do we need an EU data protection reform?*, ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm, 25 January 2012.

To transfer data on EU citizens to other jurisdictions, the jurisdiction must be recognised as providing adequate privacy protections comparable to EU standards, unless one of the exceptions applies. The European Commission makes a determination on which countries provide adequate levels of protection for the purposes of data transfers. In the absence of this, the EU has developed three mechanisms to allow cross-border flows of data[210]:

- Standard contractual clauses – these are model clauses to be inserted in contracts that set standards comparable to those in the Data Protection Directive and allow transfers of data to a jurisdiction outside of the EU even where that jurisdiction does not provide adequate protection.
- Binding corporate rules – these rules allow intra-organisational transfers of data where the company's privacy policy satisfies EU standards. They apply to multinational groups of companies allowing transfers within the group to other jurisdictions that do not have an adequate level of protection. This means that the group does not have to sign an agreement with standard contractual clauses each time it transfers personal information. The rules must be agreed by the relevant national data protection authority prior to be relied upon.
- US-EU Safe Harbor Framework – this is an agreement under which US companies self-certify that they will apply the protections under the Data Protection Directive, even though US laws are considered inadequate from an EU perspective[211]. It applies only to US companies, recognising the significant trade between the US and EU.

The Safe Harbor Framework has received criticism of its compliance arrangements, including the lack of enforcement powers of US-based regulatory bodies.[212] On 19 July 2013, the European Commissioner for Justice, Fundamental Rights and Citizenship, Viviane Reding, announced a review of the Framework, indicating that the current agreement provides a loophole for data transfers that may not adequately protect data.[213] The European Commission has undertaken an assessment of the Framework and has proposed actions for improvements to the scheme.[214]

Cybersecurity

The Council of Europe Convention on Cybercrime is the first international treaty on

---

[210] Visit ec.europa.eu/justice/data-protection/document/international-transfers/index_en.htm for more information on cross-border data flows in the EU.
[211] D C Dowling Jr, *International Data Protection and Privacy Law*, White & Case, August 2009, p. 12.
[212] Ibid, p. 16.
[213] V Reding (European Commissioner for Justice, Fundamental Rights and Citizenship), *Informal Justice Council in Vilnius*, press release, europa.eu/rapid/press-release_MEMO-13-710_en.htm, 19 July 2013.
[214] EU, *Restoring Trust in EU-US data flows - Frequently Asked Questions*, memo, http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm, 27 November 2013.

crimes committed via the Internet and other computer networks.[215] Signatories to the convention need to adopt a number of legislative and other measures regarding offences such as copyright infringement, computer-related fraud, child pornography and violations of network security. The convention was put into effect in Australia by an amendment to existing Commonwealth laws under the *Cybercrime Legislation Amendment Act 2012*, which included amendments to the *Telecommunications (Interception and Access) Act 1979*, the *Telecommunications Act 1997*, the *Mutual Assistance in Criminal Matters Act 1987*, and the *Criminal Code Act 1995.*[216] Being a party to the Convention on Cybercrime will assist Australian law enforcement agencies to obtain data about cybercrime from partner agencies from 41 other countries.[217]

The OECD has also developed guidelines on security. The Guidelines for the Security of Information Networks and Systems provide guidance to member states on anticipating risks, designing and adapting security policies and responding the threats, while also protecting individuals' rights.[218]

International standards on security have also been developed by the International Standards Organization. ISO27001 is often cited as a key security standard for cloud computing.

To assist in addressing the potential security risks associated with cloud computing, some jurisdictions have created specific programs to provide a standardised approach to secure storage of government information in the cloud. For example, in the US, the Federal Risk and Authorization Management Program (FedRAMP) provides a baseline to initiate, review, grant and revoke security authorisations for cloud services used by government agencies.[219] Similarly, in the UK cloud services can receive Pan Government Accreditation status to ensure they meet certain security requirements for the storage of government information.[220] The UK has also established G-Cloud frameworks for government procurement of cloud services and CloudStore, an online marketplace to facilitate the procurement of cloud services by government agencies.[221]

---

[215] Convention on Cybercrime, conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG, 23 November 2001.
[216] Minter Ellison, *Australia's New Cybercrime Law*, www.minterellison.com/publications/cybercrime-privacy-update-201305/, 29 April 2013.
[217] The Hon M Dreyfus QC MP, *Australia signs on to international cybercrime treaty*, media release, Parliament House, Canberra, pandora.nla.gov.au/pan/132822/20130906-1028/www.attorneygeneral.gov.au/Mediareleases/Pages/2013/First%20quarter/4March2013-Australiasignsontointernationalcybercrimetreaty.html, 4 March 2013.
[218] R Berry and M Reisman, 'Policy Challenges of Cross-Border Cloud Computing', United States International Trade Commission, *Journal of International Commerce and Economics*, May 2012, p. 18.
[219] Visit cloud.cio.gov/fedramp for more information.
[220] Visit gcloud.civilservice.gov.uk/supplier-zone/accreditation/ for more information.
[221] Visit gcloud.civilservice.gov.uk/ for more information.

Copyright

The World Intellectual Property Organization's (WIPO) Copyright Treaty and the WIPO Performances and Phonograms Treaty were established in 1996 to address the threats posed to intellectual property by rapid developments in technology.[222] Approximately 90 countries have ratified these treaties[223], including Australia. The *Copyright Amendment (Digital Agenda) Act 2000* amended the *Copyright Act 1968* to comply with the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty and address rapid developments in technology by replacing technology-specific rights with technology-neutral rights so that amendments to the Act are not needed each time there is a development in technology.[224]

Other standards

In addition to these, other international standards or codes of conduct may also have an impact on cloud computing. Standards will vary from industry to industry. An example of a standard that will have a broad impact, as it applies to businesses that store, process or transmit cardholder data is the Payment Card Industry Data Security Standard.[225] The standard is regulated by the Payment Card Industry Security Standards Council. The requirements of the standard may apply to both the customer of a cloud service and the cloud service provider, requiring both to ensure that security requirements are met. As a business that contracts a third party to store, process or transmit cardholder data on its behalf, it is important that the third party is aware of the requirements of the standard. The Payment Card Industry Security Standards Council has issued guidelines on compliance with the standard for cloud computing.

[222] World Intellectual Property Organisation Copyright Treaty, www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html, 1996.
[223] International Intellectual Property Alliance, Scorecard of WIPO Treaties Accessions/Ratifications as of October 15, 2012, www.iipa.com/pdf/2012_Oct15_Scorecard_WIPO_Treaties.pdf, 2012.
[224] Explanatory Memorandum to Copyright Amendment (Digital Agenda) Bill 2000, www.comlaw.gov.au/Details/C2004B00540/Explanatory%20Memorandum/Text, 2000.
[225] Visit www.pcisecuritystandards.org/security_standards/index.php for more information.

Attachment E: Discussion questions

Chapter 1 Questions

Are there other issues that impact on competition in the Australian cloud services market? How does the cost and complexity of Australian regulation compare to other jurisdictions?

Is there evidence of anti-competitive practices in the Australian cloud services market? If so, how could these issues best be addressed?

Are existing copyright laws impacting on the Australian cloud services market? How could any issues best be addressed?

What indicators should government consider to determine whether there are issues affecting the competitiveness of the Australian cloud services market?

Chapter 2 Questions

Are there other contractual or consumer issues affecting consumers of cloud services? How could any issues best be addressed?

Is the current coverage of consumer, telecommunications and broadcasting law appropriate? What opportunities exist to provide greater clarity for industry and better protection for consumers?

Do consumers of cloud services have sufficient confidence in the market?

Is there a need for additional measures to raise awareness among consumers on what to look for in cloud service contracts? What form could these measures take?

What indicators should government look to, as evidence that there are consumer issues (such as systemic information asymmetry) in the cloud service market?

Chapter 3 Questions

Are there other issues that affect data protection in cloud services?

Are existing privacy protections suitably tailored to cloud services? Do cloud services raise novel issues in the application of privacy law?

Are there areas of privacy law that would benefit from further clarification?

To what extent are jurisdictional differences between privacy regimes creating problems in the take up or provision of cloud services in Australia?

What are the benefits to Australian consumers in using onshore data centres? What are the benefits of offshore data centres?

What indicators should government consider to determine whether there are significant privacy concerns in the Australian cloud services market?

Chapter 4 Questions

Are there other cybersecurity issues that affect cloud computing?

Are existing laws adequate in protecting users of cloud services? What opportunities exist to promote even greater confidence in the cloud services market?

What indicators should government consider to determine whether there is a lack of adequate security in the cloud services market?

Chapter 5 Questions

How can government use of cloud services best facilitate take up among consumers?

What are the barriers to greater adoption of cloud services within government? How can these barriers be best addressed?

What indicators should government consider to determine whether the Government's use of cloud services is inhibiting take up of cloud services?

Chapter 6 Questions

How are existing government access laws impacting on the cloud services market in Australia?

Are there opportunities to lower compliance costs to industry and provide greater certainty and protection to users of cloud services?

What measures could Australia undertake internationally to improve trust and confidence?

What indicators should government look to, to determine whether government access laws are negatively impacting on the Australian cloud services market?

Chapter 7 Questions

What impact is red tape having on the cloud services market in Australia?

How do the compliance obligations imposed by Australian law compare to other jurisdictions?

How well is the current regulatory environment understood by the market?

What opportunities exist to reduce compliance costs for cloud service providers and users of cloud services?

What non-regulatory actions could government undertake to encourage the take up of cloud services? Should there be a focus on highly regulated markets?

What indicators should government consider to determine whether there is over-regulation in the cloud service market?

Attachment F: Acknowledgements

The Department would like to acknowledge the following organisations for their valued contributions to the development of the Cloud Computing Regulatory Stock Take.

- **Australian Information Industry Association**
- **National Standing Committee on Cloud Computing[226] and Global Access Partners**
- **Australian Computer Socierty, Special Interest Group**
- **Amazon Web Services**
- **Ashurst**
- **Australian Communications Consumer Action Network**
- **Business Software Alliance**
- **Communications Alliance**
- **Corrs Chambers Westgarth**
- **Information Integrity Solutions**
- **Internet Industry Association**
- **Microsoft**
- **NextDC**
- **SAP**
- **Telstra**
- **University of Melbourne**

[226] See http://www.globalaccesspartners.org/LiteratureRetrieve.aspx?ID=119838